REPUBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD DE LOS ANDES
FACULTAD DE INGENIERÍA
MAESTRIA EN COMPUTACIÓN

MODELO PARA LA AUDITORÍA DE LA SEGURIDAD INFORMÁTICA EN LA RED DE DATOS DE LA UNIVERSIDAD DE LOS ANDES

TESIS PRESENTADA COMO REQUISITO PARA OPTAR AL GRADO DE MAGISTER EN COMPUTACIÓN

AUTOR: REINALDO N. MAYOL ARNAO
TUTOR: PROF. JACINTO DAVILA, PhD

MERIDA, MARZO 2006

A mis padres, inmenso caudal del que se desprendió el riachuelo que es mi vida

A Solbey y Camila por ser el viento que me empuja, por la confianza, por la frescura y por el amor

Gracias a Jacinto por la paciencia y la voluntad cerradora.

A la utilidad de la virtud

Índice de contenido

Índice de ilustraciones

Índice de tablas

Resumen

Auditar, de manera correcta, los mecanismos de seguridad utilizados en el ofrecimiento de los servicios de Tecnologías de Información (IT) es uno de los elementos fundamentales para el éxito de esta labor. El término Auditar Correctamente incluye varios elementos importantes, uno de ellos es contar con un modelo de auditoría completo, equilibrado y técnicamente correcto. Este documento propone un modelo de auditoría de la seguridad informática para aquellos servicios de IT que se ofrecen por RedULA para la Universidad de Los Andes, extensible para cualquier entidad de características similares.

Introducción

La red de datos de la Universidad de Los Andes (en lo sucesivo RedULA) ha venido creciendo de manera significativa en la última década, hasta convertirse en patrón de referencia dentro de las instituciones universitarias, no sólo a nivel nacional sino también en el entorno latinoamericano. Junto con el crecimiento físico de la red, lo han hecho también los servicios que se ofrecen utilizándola como plataforma de transporte. Con una red tan extendida, tecnológicamente diversa y con una variedad significativa de actores, servicios y usuarios, es fácil que comiencen a ocurrir errores y desviaciones que pueden comprometer la propia subsistencia de la red como un entorno efectivo de trabajo. Esta realidad impone la necesidad de realizar procesos de auditoría del funcionamiento de la red que permitan detectar problemas graves , establecer patrones de comportamiento, realizar planificación de crecimiento e incluso detectar problemas incipientes que pudiesen poner en riesgo la operación futura de la red.

Durante los últimos 18 meses RedULA ha sido objeto de un proceso de auditoría externa mediante la cual se ha hecho evidente que el tema de Seguridad Informática es uno de los que mayor repercusión e importancia tiene para la operación cotidiana. Desde los primeros procesos de auditoría se detectó que, en todas las áreas que fueron auditadas, la situación referente a las condiciones para establecer un entorno adecuado de Seguridad Informática eran deficientes y este acápite fue catalogado como uno de los más críticos de los auditados.

A la situación expresada en el párrafo anterior debe sumársele el incremento significativo de los incidentes de seguridad informática[1] a nivel de toda la Internet, sus usuarios y sus aplicaciones. Este incremento puede achacársele a varios factores, además del crecimiento de la red de datos, el número de servicios y la cantidad de usuarios, también son responsables las malas prácticas de desarrollo de software, las instalaciones defectuosas, la subestimación de los riesgos reales y la sobrestimación de otros, la falta de compromiso organizacional con el mantenimiento de los niveles mínimos de seguridad informática y la proliferación de soluciones propietarias que imponen "estándares" de uso, desarrollo y explotación sin tener en cuenta los elementos de seguridad.

El incremento de los incidentes de seguridad informática ha sido tal que, organizaciones como Computer Emergency Response Team (CERT) han dejado de publicar desde el año 2003 estadísticas sobre el número de incidentes, reconociendo la incapacidad de ofrecer datos reales sobre el tema. En

[1] Un incidente de seguridad puede definirse como un evento, que fuera del control de quien lo padece, pone en riesgo la integridad, confidencialidad o disponibilidad de la información. Aunque no suele mencionarse, debido a que se obtiene como un "subproducto" de los procesos para garantizar los aspectos antes señalados, la autenticidad (de la información, del origen y del destino de la misma y los actores involucrados) es otro de los elementos que deben resguardarse.

RedULA se detectan diariamente unos 22000 intentos serios[2] de intrusión desde el exterior. Si se toman como válidos los valores comúnmente aceptados sobre la proporción de incidentes de fuentes internas y externas puede estimarse que el número total de incidentes diarios puede estar rondando los 100.000.

La Universidad de Los Andes no es única en esta situación. El más reciente informe 2004 E-Crimen Watch Survey [ECRIMW] refleja que las pérdidas asociadas a incidentes de seguridad en el año 2003 llegaron a los 600 Millones de dolares (sólo en EE.UU). Otros datos importantes de este informe son los siguientes: el 43 % de las empresas encuestadas ha reportado un aumento de los incidentes de seguridad con respecto al año 2002, mientras que el 70 % de las empresas encuestadas reporta al menos un incidente de seguridad en el año.

La misma encuesta mencionada anteriormente categoriza los niveles de impacto de la siguiente forma: El 56 % de los encuestados declaró que las mayores pérdidas están asociadas a fallas operacionales, el 25 % declara pérdidas financieras. La mitad de los encuestados declaró no poseer mecanismos para cuantificar sus pérdidas y el 41 % indicó no poseer planes para enfrentar incidentes asociados a la seguridad informática.

Durante el último año, el proceso de auditoría de la Seguridad Informática de RedULA se ha llevado a cabo de manera más bien empírica, por un equipo liderado parcialmente por el autor de este documento, siguiendo métodos que no se ajustan del todo a las necesidades, requerimientos y particularidades de la organización. La ausencia de un modelo sólidamente desarrollado también frena el desarrollo del propio proyecto de auditoría, al impedir su diversificación y crecimiento debido a la dependencia los resultados de los conocimientos, experiencia y métodos de trabajo del personal que labora en el proyecto.

Más de un año después de haber comenzado el proceso de auditoría de los servicios de RedULA se han obtenido grandes éxitos al incidir en las decisiones de corrección de situaciones críticas en varias redes que conforman RedULA, tales como la red del Rectorado. Sin embargo, también han quedado en evidencia deficiencias y limitaciones de la forma en que se audita actualmente.

En el trabajo que se describe en este documento, se ha creado un modelo para la auditoría de Seguridad Informática de la Red de Datos de la Universidad de Los Andes y algunos de los servicios fundamentales que se ofrecen sobre la misma (web hosting, conectividad, control de acceso, correo electrónico). El modelo consta de una descripción general del cómo se debe proceder para hacer una auditoría de seguridad, tomando en cuenta las peculiaridades de nuestra organización. Así, el modelo incluye reglas para guiar la conducta del personal en la auditoría de otros aspectos importantes como las políticas de seguridad, las condiciones de seguridad física, las pruebas de penetración y los sistemas de detección de intrusos.

[2] En este número se descartan incidentes asociados a errores de configuración, virus informáticos o mala operación de los medios de cómputo. Este número sólo se refiere a incidentes cuyo objetivo puede ser claramente establecido como un ataque a la confidencialidad , disponibilidad y autenticidad de los medios de cómputo y los datos que manejan. Dato tomado de las estadísticas de los sistemas de detección de intrusos de RedULA.

Este trabajo no pretende cubrir todos los temas que deben ser objeto de esfuerzo para garantizar un entorno seguro de operaciones en RedULA, como primer paso hemos escogido aquellos aspectos que en son de mayor relevancia e impacto. Hablamos de un modelo y no de una metodología, porque no hemos pretendido que la misma estrategia se pueda aplicar en cualquier otro caso o tipo de organización sometida a este tipo de auditorías. Lo que sí hemos pretendido, y mostramos evidencia de haberlo logrado, es mejorar significativamente nuestra capacidad y aptitud institucional para auditar la seguridad informática.

Este documento se encuentra divido en 4 capítulos y varios anexos. El primer capítulo describe la situación que dio origen al presente trabajo. El capítulo 2 se dedica a la descripción funcional del modelo propuesto y de cada uno de los elementos que lo conforman. El capítulo 3 constituye el centro del trabajo y se dedica a la exposición completa del modelo. En el capítulo 4 se refiere a la prueba del modelo propuesto y su comparación con el esquema de auditoría que actualmente se utiliza, en el se exponen los resultados obtenidos de la ejecución de un proceso de auditoría utilizando el modelo propuesto.

Si el lector utiliza una versión digital de este documento podrá utilizar hipervínculos . Haciéndolo podrá moverse entre los diferentes módulos que conforman el modelo, entre la explicación de cada módulo y el código del mismo y hacia los anexos de información cuando estos son referenciados. Los anexos tienen nombres que puedan ayudar al lector a encontrar el objetivo de los mismos, así en lugar de simplemente colocar un número, el lector encontrará nombres como FIREWALLS identificando que se refiere a alguna pieza de esa tecnología.

Capítulo 1. Planteamiento del Problema

La Corporación Parque Tecnológico de Mérida (en lo sucesivo CPTM) administra parte de la infraestructura de Tecnologías de Información (en lo sucesivo TI) de la Universidad de Los Andes. Buscando mejorar la calidad de los servicios ofrecidos se ha creado el Proyecto de Auditoría Informática el cual, entre otros aspectos, debe realizar procesos de auditoría a la seguridad de los servicios de TI. Para poder realizar un proceso de auditoría permanente, independiente y estable es necesario contar con un modelo de auditoría que tome en cuenta los elementos particulares del ambiente universitario, del tipo de servicio que se ofrece y de sus necesidades reales de seguridad informática.

Con este trabajo se ha pretendido crear un modelo de auditoría de seguridad informática para los servicios de Tecnologías de Información ofrecidos por la CPTM a la Universidad de Los Andes. El uso de modelos durante el proceso de auditoría es importante, no sólo para garantizar la consecución de resultados correctos y completos, sino también para garantizar que un equipo de profesionales obtenga un resultado homogéneo, reduciendo la importancia de los niveles de pericia, instrucción, audacia, conocimiento de la organización auditada, relación con los auditados, experiencia y otros del auditor. Por tal razón, resulta común el uso de modelos en empresas auditoras y consultoras profesionales, desarrollados por expertos para conseguir resultados homogéneos con equipos de trabajo que no lo son.

Otro elemento importante a favor del uso de los modelos de trabajo en el campo de la auditoría es garantizar la obtención de resultados correctos y completos en tiempos adecuados de acuerdo a las condiciones en que se realiza la auditoría.

En la actualidad existe una gran diversidad de modelos de auditoría de la seguridad informática, todos desarrollados para contextos particulares o de carácter tan general que sólo constituyen un marco referencial para el desarrollo de un proceso auditor. Las grandes organizaciones privadas de auditoría tienen siempre los suyos propios y estas constituyen un patrimonio importante de las mismas, el cual resguardan celosamente de la competencia. En el mundo de la auditoría de seguridad se dice comúnmente que una organización es lo que sus metodologías le permiten ser.

RedULA, como hemos mencionado anteriormente, no posee un modelo desarrollado para ejecutar los procesos de auditoría que adelanta, de ahí la importancia del modelo que se propone en este trabajo.

1. Objetivo Generales de la Propuesta

Diseñar un modelo para realizar auditorías de seguridad informática en ambientes universitarios, y probar el modelo sobre la infraestructura de teleinformación de la Universidad de Los Andes.

2. Objetivos Específicos de la Propuesta

- Definir las especificidades para los ambientes públicos y académicos, específicamente para RedULA de los servicios de Seguridad Informática a fin de elegir los servicios y las tecnologías candidatas a integrar el modelo de auditoría.
- Diseñar el modelo de auditoría para los servicios a ser auditados mediante revisiones de servidores y equipos de comunicaciones.
- Diseñar el modelo de auditoría para los servicios a ser auditados mediante pruebas de penetración.
- Diseñar las reglas para ponderar referencialmente (en el capitulo 2 mencionaremos los detalles tomados en cuenta para elaborar la necesaria ponderación para las pruebas) la importancia de las condiciones de riesgo detectadas según su nivel de impacto y el activo que afecten.
- Probar el modelo en la plataforma universitaria.

3. Alcance de la Propuesta

El modelo general que se propone debe ser utilizado para la auditoría de seguridad informática de los servicios de TI de la Universidad de Los Andes, específicamente para aquellos que ofrece RedULA a través del CPTM.

El modelo constituye una guía referencial para la realización de procesos de auditoría que utilicen las siguientes tipos de pruebas, los cuales, según la opinión y experiencia del autor son las más comunes:

- Revisiones: Se refiere a verificaciones de los parámetros de seguridad realizadas directamente en los servidores, estaciones de trabajo y equipos de comunicaciones sin violar los mecanismos de seguridad, buscando condiciones de instalación que pudiesen favorecer la consumación de condiciones de Negación de Servicios. Ej.: Espacios de discos insuficientes, cargas elevadas de uso de memoria o CPU, instalaciones incorrectas de servicios, etc.

- Entrevistas: Se refiere a sondeos realizados a usuarios y administradores para encontrar dentro de las políticas, normas y procedimientos (formalmente establecidas o "de facto") condiciones que pudiesen producir afectación a la seguridad informática de los servicios.

- Pruebas de Penetración: Se refiere al conjunto de pruebas intrusivas realizadas para tratar de vulnerar los sistemas de seguridad, escalar los privilegios de atacante y eventualmente poner en riesgo la integridad, confidencialidad y disponibilidad de la información o de los sistemas de seguridad de la organización. Las pruebas de seguridad se realizan en dos escenarios: desde el interior de la ULA, en este caso se habla de pruebas internas o desde el exterior, pruebas externas.

Esta propuesta no incluye el diseño de modelos para la realización de auditoría a servicios ofrecidos por terceros, aún cuando estos pudiesen ser utilizados para el acceso a los servicios de RedULA. Ej. Proveedores de Servicios Externos, etc.

Como resultado de la ejecución de este trabajo se ha obtenido un grupo de reglas que sirven como guía metodológica para la ejecución de los procesos de auditoría en las condiciones que se han expuesto anteriormente.

4. Trabajo Ejecutado

- Definir los servicios de TI candidatos a ser auditados.
- Definir los parámetros de seguridad informática a auditar en equipos servidores.
- Definir los parámetros de seguridad informática a auditar en equipos clientes.
- Definir los parámetros de seguridad informática a auditar en equipos de telecomunicaciones.
- Definir los parámetros a auditar en los equipos de seguridad.
- Definir los elementos a evaluar mediante entrevistas y sondeos a los usuarios de los servicios de TI.
- Definir el alcance de los procesos de auditoría para cada uno de los servicios de TI seleccionados.
- Diseñar el modelo de auditoría para cada uno de los servicios a ser auditados en servidores.
- Diseñar el modelo de auditoría para cada uno de los servicios a ser auditados en estaciones de trabajo.
- Diseñar el modelo de auditoría para cada uno de los servicios a ser auditados en equipos de telecomunicaciones.
- Diseñar el modelo de auditoría para cada uno de los servicios a ser auditados los equipos de seguridad.
- Establecer los criterios para la ponderación referencial de los resultados de cada proceso de auditoría de los servicios seleccionados.
- Probar el modelo diseñado.

Capítulo 2. Fundamentos Teóricos del Modelo Propuesto.

1. Situación Actual de la Seguridad Informática en la Universidad de Los Andes.

RedULA no fue concebida, ni ha sido operada (hasta hace muy poco), pensando en la seguridad de sus componentes o las aplicaciones que sobre ella se ejecutan. Durante mucho tiempo, el énfasis del desarrollo de la red, como de la mayoría de las redes de su tipo a nivel internacional, estuvo centrado en su crecimiento. Esta situación se agrava si se toma en cuenta las características de uso de la red, en la cual deben coexistir servicios administrativos fundamentales para el desarrollo de la vida universitaria y los necesarios procesos de experimentación, investigación y desarrollo propios de una institución académica.

El problema más común que deben enfrentar los administradores de la seguridad de RedULA es la incidencia de virus informáticos cuyas características afectan directamente el comportamiento de la red (ej. generando grandes cantidades de datos que degradan el rendimiento de la red.). Esta situación es realmente grave y se enfatiza por las costumbres de uso, el tipo de sistema operativo y la cantidad de equipos clientes existentes en la universidad e interconectados por RedULA. RedULA toma en estos momentos algunas medidas para intentar minimizar la incidencias de virus (y planea otras a mediano plazo). Sin embargo, dichas medidas nada pueden hacer para impedir que los computadores personales se continúen infectando por medios diferentes a la red y terminen afectándola. Es de esperar que con el aumento de sistemas operativos distintos a Windows disminuya el efecto de los virus. Sin embargo, toda vez que su reemplazo por otros los sistemas operativos no hace imposible la proliferación de virus, esta no puede ser tomada como una solución definitiva a este problema.

Otro problema común se debe a intrusiones en las estaciones de trabajo de los usuarios y en servidores débilmente configurados. En este sentido una de las labores fundamentales de los administradores de seguridad consiste no sólo en detectar y detener las intrusiones sino en incidir directamente sobre la causa del problema, como hemos dicho: la falta de cultura y pericia de quienes como administradores o como simples usuarios usan los sistemas.

La administración de la red no está exenta de estas carencias de pensamientos y habilidades referentes a la seguridad, por tal razón también los sistemas operados por RedULA se han visto afectados e incluso todavía no se tienen en cuenta muchos elementos de seguridad al establecer y operar algunos servicios. La plataforma de seguridad es todavía incipiente e inestable . Sólo unos pocos servicios y sitios son supervisados de forma continua y completa y pocos son los sitios de control establecidos. Adicionalmente existe una inmensa plataforma de equipos de comunicaciones (routers, switches, concentradores, equipos inalámbricos,etc) instalados y operados sin cumplir con los requerimientos de seguridad, la mayoría de ellos incluso, incapaces técnicamente de hacerlo.

Muchos de los servicios académicos y administrativos que se ofrecen tienen serias deficiencias desde el punto de vista de seguridad. Cada vez más, nuevos servicios se establecen utilizando la red como mecanismo de transporte. Ya, dentro de la universidad, se han vivido experiencias del impacto que puede tener sobre un servicio el no protegerlo adecuadamente o no tomar en cuenta los elementos de seguridad en su diseño, implantación y explotación. Si unimos la tendencia creciente a aumentar los servicios en red con una tendencia similar a aumentar los incidentes de seguridad, el único camino es comenzar a preocuparse y actuar en función de mejorar las condiciones de seguridad de RedULA.

Actualmente RedULA recibe una gran cantidad de ataques desde el exterior, una proporción aún mayor ocurren desde el interior de la propia red. A modo de ejemplo, tal y como se mencionó anteriormente, los servicios de filtrado de borde actualmente detectan cerca de 22000 intentos de acciones que pueden considerarse intrusivas. Entre las más significativas se encuentran los intentos de enumeración de la red, de un servidor o servicio específico, los intentos de acceso con identidades falsas y de adivinanza de contraseñas y las tentativas de realizar operaciones aún más agresivas como ataques de Negación de Servicios o de explotación de debilidades de los sistemas instalados. Otro dato es revelador de la situación en seguridad informática de la universidad; en promedio, diariamente una estación cliente da señales de haber sido comprometida por atacantes externos o internos. El término comprometida significa que existen evidencias suficientes de que el sistema operativo ha sido violentado y la estación responde ahora a las órdenes del atacante, lo hace de manera anárquica o incluso se ha perdido la información contenida en ella.

Ante esta realidad hay varios caminos no excluyentes a seguir. El primero es crear la cultura de la seguridad no sólo entre quienes tienen que encargarse de la administración de los servicios, sino también entre los usuarios de los mismos. Otra labor es mejorar las condiciones en que en la actualidad se administran y diseñan los sistemas y, obviamente, corregir las condiciones deficientes de seguridad y velar porque al hacerlo no se creen otras condiciones de riesgo. Para esta última labor las funciones de auditoría son imprescindibles.

Pero para que un proceso de auditoría tenga resultados completos, normalizados y correctos debe contar con una guía metodológica [HMATS]. Como hemos mencionado actualmente se utiliza un esquema de pruebas que no ha sido concebido ni adecuada a las necesidades y características de RedULA. Como resultado de esto gran cantidad de elementos importantes no son auditados, los resultados no son homogéneos y la relación del equipo de servicios con el auditor puede influir en los resultados En el capitulo 4 se muestra una comparación cuantitativa entre el modelo que se propone con este trabajo y el que se utiliza en la actualidad.

El modelo que se propone ha sido concebido teniendo en cuenta tanto las características de RedULA, como los servicios más importantes y vulnerables. La siguientes secciones describen las características generales del modelo propuesto, el lenguaje en que ha sido escrito y la forma de uso del mismo.

2. Descripción del Modelo Propuesto.

Como dijimos, el modelo es una descripción general del cómo se debe proceder para hacer una auditoría de seguridad y, consecuentemente, está constituido por grupos de reglas agrupadas en módulos, para guiar la conducta del personal encargado de la auditoría. A continuación se le describe en detalle:

2.1 Estructura detallada del modelo

La estructura del modelo propuesto ha sido establecida siguiendo la forma común de realizar un proceso de auditoría, específicamente uno de Seguridad Informática. Existen 4 módulos. Estos son:

A) Definición de las condiciones para la auditoría.
B) Definición de las características técnicas
C) Pruebas de Penetración
D) Revisiones de las configuraciones.

En el acápite 2.4 de este capítulo detallaremos los objetivos y el alcance de cada módulo. Mientras nos concentraremos en los detalles de la estructura del mismo.

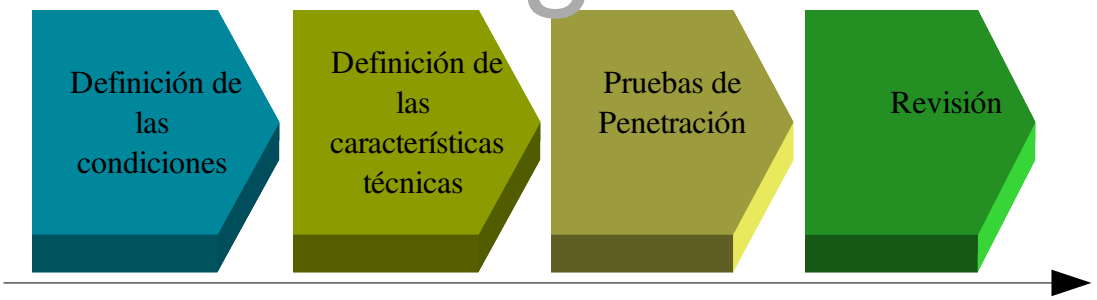


Ilustración 1: Módulos que conforman el modelo propuesto.

Todos los módulos funcionan como un sistema, dando de conjunto una visión general de la seguridad informática del sitio auditado. Cada módulo está compuesto por secciones. Las secciones a su vez se conforman por reglas. Una regla está especificada por un conjunto de pruebas. El orden en que se ejecuten las secciones dentro de un módulo normalmente no es significativo, cuando no lo es, el sistema explícitamente señala los elementos prelatorios. El orden en que se ejecutan las pruebas y las reglas dentro de una sección suele ser significativo. Dentro de un módulo el auditor tiene libertad de ejecutar o no una sección de acuerdo a varios factores, entre ellos el objetivo de la auditoría o las

características técnicas de la plataforma que se audita.

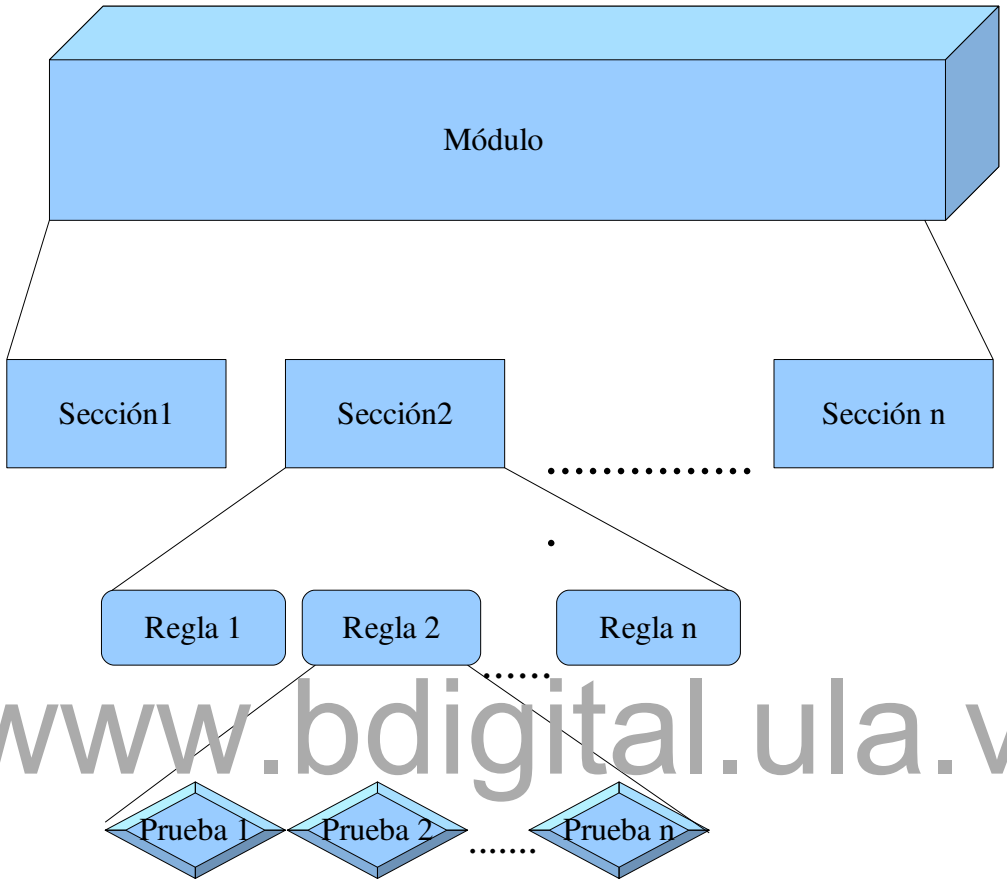


Ilustración 2: Estructura de un módulo

La ilustración número 3 muestra un ejemplo más en detalle. Más adelante en este acápite nos referiremos a la sintaxis de los elementos que conforman el modelo.

Cada módulo debe tener valores de salida y puede tener algunos de entrada. La entrada es la información usada en el desarrollo de cada tarea. La salida es el resultado de las secciones completadas. La salida puede o no ser datos analizados para servir como entrada para otro módulo, recomendaciones que conformarán el informe final o simplemente datos que soporten las recomendaciones . Puede ocurrir que la salida de un módulo sirva como entrada para más de un módulo o sección. Ej. La definición del espectro de direcciones IP a auditar sirven de entrada para varias otras secciones correspondientes a otros módulos.

Como regla general todo módulo debe tener valores de salida[HMATS]. Un módulo sin salidas puede

significar una de tres cosas:

- Las pruebas no fueron ejecutadas apropiadamente.
- Las pruebas no se aplicaban.
- Los datos resultantes de las pruebas se analizaron inapropiadamente.

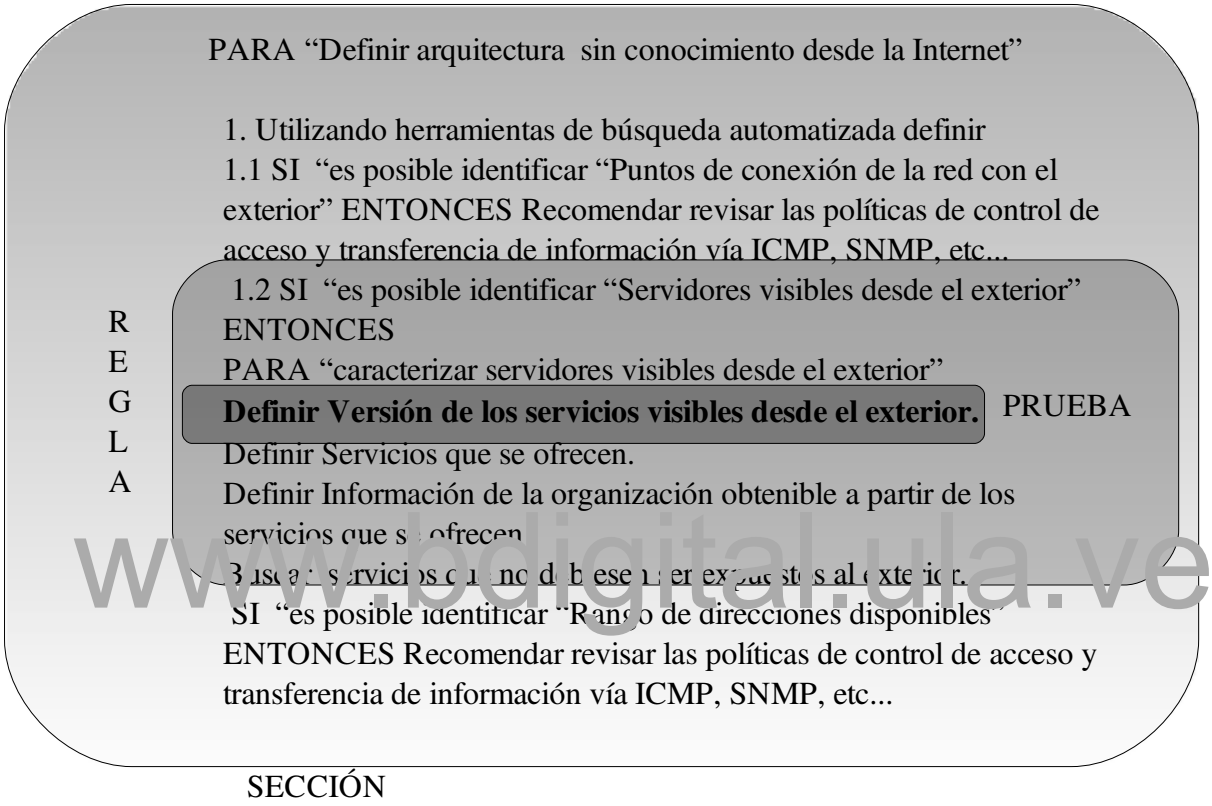


Ilustración 3: Una sección del modelo conformada por varias reglas y pruebas

El modelo fluye desde el módulo inicial hasta completar el módulo final y permite la separación entre recolección de datos y pruebas de verificación de y sobre los datos recolectados. Cada módulo puede tener una relación con los módulos adyacentes. Cada sección puede tener aspectos interrelacionados a otros módulos y algunas se interrelacionan con todas las otras secciones. Durante la ejecución de cada regla, o incluido de una prueba, se van emitiendo las recomendaciones que conformarán el informe final. Por ejemplo en el segmento de código mostrado en el ejemplo de la ilustración 3 puede leerse la siguiente recomendación: *Recomendar revisar las políticas de control de acceso y la transferencia de información...*

2.2 Ponderación de los Resultados

Una entidad auditada estará muy interesada en obtener, como resultado del proceso de auditoría, un listado completo de las condiciones de riesgo a las que está sometida su infraestructura de información. Sin embargo, es también muy importante definir cuantitativamente el peso específico de cada condición hallada. Como es de suponer no todos las vulnerabilidades, errores y otras condiciones significan igual nivel de riesgo para la integridad, disponibilidad y confidencialidad de la información y los medios que la soportan.

Esta ponderación es de suma importancia para la definición del necesario proceso ulterior de correcciones, toda vez que siempre debe comenzarse por aquellas condiciones que impliquen mayor nivel de riesgo. La ilustración no. 4 muestra la relación entre el orden en que deben ejecutarse las correcciones y el nivel de riesgo que las vulnerabilidades encontradas tienen. Como se muestra en la ilustración las vulnerabilidades (marcadas como puntos blancos) que se encuentran dentro del rectángulo rojo deben ser las primeras a ser corregidas toda vez constituyen los mayores riesgos.

Establecer niveles de ponderación para cada prueba suele ser un proceso mas complejo de lo que parece a primera vista, debido al nivel de subjetividad que puede acarrear y la los múltiples factores que deben tomarse en cuenta (por ejemplo lo que es muy crítico para una organización puede no serlo para otra). Para hacerlo nos hemos basado en dos fuentes y tratado de conjugar sus resultados. La primera ha sido la categorización de los resultados que comúnmente hacen las herramientas de búsqueda de vulnerabilidades automatizadas (alto , medio y bajo). La segunda fuente fue la Metodología Abierta para Pruebas de Seguridad[HMAST].

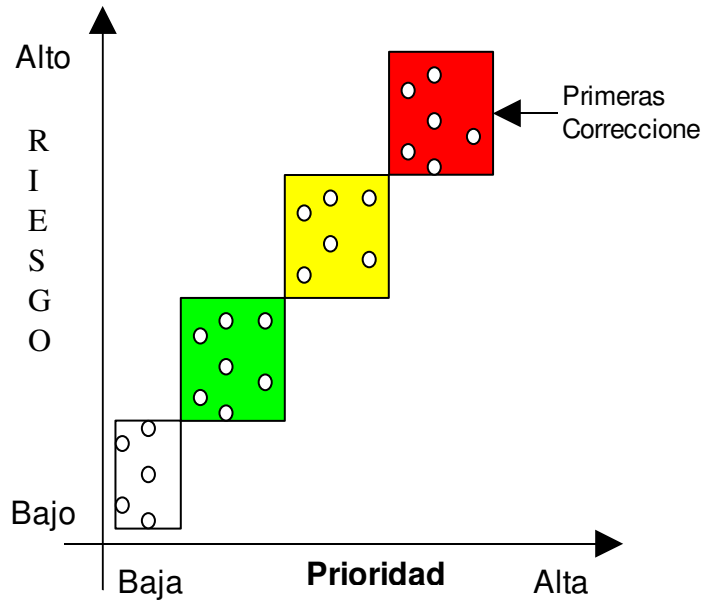


Ilustración 4: Ponderación de los resultados y su relación con el orden de las correcciones

Siguiendo ambos criterios hemos categorizado los riesgos (no el impacto del cual hablaremos más adelante) siguiendo el siguiente esquema[HMAST]:

- ***Vulnerabilidades****: Se refiere a una falla inherente a las características de diseño o creación al propio sistema y no achacable a mala implantación o manejo por parte de cualquiera.*
- ***Debilidad****: Se refiere a una falla no achacable al producto que se evalúa sino al ambiente que lo sostiene o que cohabita con él.*
- ***Filtrado de Información****: Se refiere a una falla inherente en el mecanismo de seguridad mismo que permite el acceso privilegiado a información sensible o privilegiada acerca de datos.*
- ***Preocupación****: Se refiere a un evento de seguridad que puede resultar al no seguir las prácticas recomendadas de seguridad, y que por el momento no se presente como un peligro real.*

Otro factor importante ha sido tomado en cuenta obtener un resultado final de ponderación: El riesgo real que una determinada condición produzca sobre la confidencialidad, integridad y disponibilidad de la información o las aplicaciones que la soportan. Antes de continuar es necesario dar definiciones de lo que a afecto de este documento significan estos tres términos.

- Confidencialidad: La confidencialidad o privacidad [...] se refiere a que la información sólo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: las líneas "pinchadas" la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.[BORCSI]

- Integridad: La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

- Disponibilidad: La disponibilidad de la información se refiere a la seguridad de que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Asociado a estos tres conceptos básicos está el de autenticidad y relacionado a este el término no repudio. La autenticidad puede definirse como la seguridad que el origen o destino de la información y la información misma no han sido alterados y que existen mecanismos para detectar de manera inequívoca una suplantación ya sea de la información o de los actores que participan en el acto de comunicación, distribución o almacenamiento de la misma. El término no repudio se refiere a la capacidad de determinar de manera inequívoca la autoría de una determinada acción.

Con estos elementos hemos decidido categorizar la importancia de las condiciones de riesgo de la siguiente forma:

Nivel de Riesgo	Significado
Bajo	Se refiere elementos que se ubiquen dentro de la categoría de Preocupación y que de materializarse no pongan en riesgo real la integridad, confidencialidad y disponibilidad de la información. Ej. Utilización de protocolos de cifrado débiles para comunicaciones no críticas.
Medio	Se refiere a elementos que se ubiquen en las categorías Filtrado de Información ó Debilidad, siempre y cuando no produzcan de manera inmediata condiciones que pongan en riesgo la integridad, confidencialidad y disponibilidad de la información. Ej. Dispositivos con la comunidad de lectura SNMP[3] disponible, toda vez que se trata sólo de lectura y requiere dispositivos y habilidades especiales para su explotación además de poder ser limitado su alcance por otras vías.
Alto	Se refiere a elementos que se ubiquen en cualquiera de las 4 categorías(Vulnerabilidad, Debilidad Filtrado de Información ó Preocupación), siempre y cuando produzcan de manera inmediata condiciones que pongan en riesgo la integridad, confidencialidad y disponibilidad de la información. Ej. contraseñas débiles para el acceso a dispositivos de comunicaciones críticos.

Tabla 1: Significado de los Niveles de Riesgos referenciales utilizados en el modelo propuesto

Veamos un ejemplo tomado de la sección Sendmail del módulo Revisiones:

1 PARA "Verificar la efectividad y seguridad de las técnicas de prevención de ataques del tipo DoS"

*1.1 Verificar opción **MaxDaemonChildren**. SI "la prueba falla[4]" ENTONCES Recomendar corregir esta situación.*

[3] SNMP: Simple Network Managements Protocol.

[4] Falla de la prueba significa que el número de demonios que manejan sendmail no está de acuerdo al flujo real de mensajes del servidor.

Esta prueba se refiere a la cantidad de procesos hijos que inicia el servidor SMTP[5] (Sendmail en este caso), este parámetro es esencial para evitar ataques de Negación de Servicios[6] . Como quiera que los resultados de agotar los recursos del sistema llevan a su paralización, se puede realizar con medios sencillos (en este caso basta un simple programa que de manera insidiosa y regular genere correos) y no hacen falta conocimientos especiales de la arquitectura del sitio auditado ni herramientas o pericias especiales; la condición de riesgo que describe esta prueba ha sido catalogada de ALTO RIESGO.

Las ponderaciones que se ofrecen en el modelo (pueden encontrarse las ponderaciones de cada prueba en el anexo PONDERACION) son puramente referenciales. El auditor tiene capacidad de variar la ponderación sugerida para una prueba debido a condiciones específicas del sitio a auditar o de las propias condiciones en que se ejecuta la prueba. Por ejemplo, transmitir datos críticos sin cifrar a través de la red puede considerarse como una condición de alto impacto debido a la posibilidad de que alguien acceda físicamente al medio y "escuche", cambie o destruya la información mientras viaja por la red, sin embargo, esta ponderación pudiese variar si acceder a los medios de transmisión, los extremos de comunicación o cualquiera de las partes por donde viaja la información es físicamente prohibitivo. La ponderación de los niveles se riesgo ha sido establecida por cada prueba, entendiendo que la ponderación del resto de las unidades superiores en que ha sido dividido el modelo (módulos, secciones y reglas) puede obtenerse a partir de estas.

2.3 Del lenguaje en que se ha escrito el modelo

A sabiendas de que la base conceptual es amplia, la cantidad de reglas es extensa y muchas veces requiere conocimientos específicos de herramientas, técnicas e incluso cierto nivel de experiencia y habilidades, hemos tratado de mantener el lenguaje con la mayor sencillez posible.

El modelo está formado no por una serie de acciones que se deben seguir como una receta, sino por un conjunto de funciones individuales, casi siempre correspondientes a una sección o incluso a una regla que pueden ser utilizados libremente por el auditor, siempre y cuando cumpla los requerimientos de entrada de datos de la función.

[5] SMTP: Simple Mail Transfer Protocol

[6] Ataques de Negación de Servicios (DoS en Inglés) Este es el tipo de ataque más peligroso y difícil de detener a que se puede enfrentar un administrador de seguridad. Se basa en agotar los recursos del sistema atacado solicitando más servicios que los que este está preparado para entregar. Como muchas veces se trata de peticiones idénticas a las legitimas es muy difícil separar las que forman parte del ataque de las que no.

La sintaxis utilizada es la siguiente:

***PARA** "Objetivo" "acciones"*

***SI** "Condición" **ENTONCES** "Acciones o Conclusiones" [**DE LO CONTRARIO** "Acciones o Conclusiones"]*

Se han subrayado las palabras reservadas por el lenguaje para que no sean confundidas con parte del texto descriptivo. Las acciones pueden ser reglas o llamadas a otras secciones o simplemente una prueba.

Por objetivo se entiende la meta que se busca alcanzar al realizar una determinada acción. Una condición es uno o varios elementos que deben ser evaluados previamente y que definen el ambiente de ejecución de las acciones que siguen. Una condición puede definir la pertinencia de la ejecución de una acción ulterior. Las conclusiones se refieren a las recomendaciones que el resultado de la ejecución de una acción indican y que deben ser parte del informe final. Los elementos encerrados entre corchetes son opcionales.

Una acción pueden ser grupos de subtareas o acciones individuales. Las subtareas pueden encontrarse inmediatamente en la sección o ser llamadas a otras funciones incluso fuera del módulo que se ejecuta.

Veamos nuevamente el ejemplo utilizado anteriormente identificando cada una las partes de la sintaxis descrita.

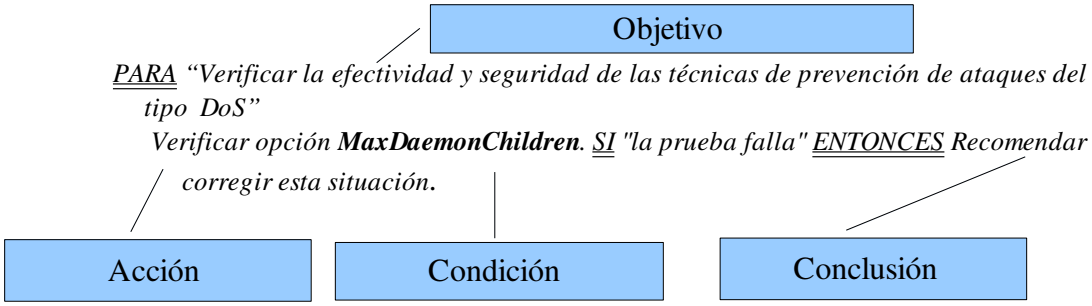


Ilustración 5: Ejemplo de la sintaxis utilizada en el modelo propuesto

Especial atención merece la expresión *si la prueba falla*. Cada prueba define condiciones diferentes para la falla o éxito de la misma. El modelo define condiciones positivas y negativas, es decir se busca guiar al auditor para verificar la existencia de los elementos mínimos imprescindibles para garantizar la seguridad y a su vez descartar elementos que no deben estar presentes. Por tal razón, las condiciones

son particulares para cada prueba. Todas las condiciones de este tipo tienen una referencia que da algunos criterios para que el auditor defina el éxito o no de la prueba. Si volvemos al ejemplo que nos ha servido de referencia podemos ver que la referencia dice: *Falla de la prueba significa que el número de demonios que maneja sendmail no está de acuerdo al flujo real de mensajes del servidor.*

Como puede observarse, los criterios que se dan para definir la falla o no de una prueba son referenciales. No puede ser de otra forma. Las valores que sirven para una condición pueden ser insuficientes para otra. Por esa razón nos hemos limitado, en la mayoría de los casos, a dar los criterios para que sea el auditor quien defina, de acuerdo a múltiples factores que dependen de las condiciones en que ejecuta la auditoría.

Existe otro tipo de referencias más específicas. Por ejemplo en la misma sección Sendmail del módulo Revisiones la referencia número 183 dice: *Cualquier versión anterior a 8.9.3 debe ser completamente sustituida, no vale la pena auditar.* En este caso la referencia establece una condición obligatoria que debe ser seguida por el auditor y que no puede ser cambiada por ninguna condición especial; toda versión de Sendmail anterior a 8.9.3 tiene suficientes errores como para que la recomendación inmediata e ineludible sea su sustitución.

El uso de referencias facilita la sencillez del lenguaje en que se ha escrito el modelo sin permitir que se pierda riqueza y profundidad en los criterios que ayuden al auditor. No hay que olvidar que el modelo no pretende ser una recopilación completa de conocimientos ni una receta exacta y de bajo nivel de auditoría sino una guía para la ejecución de procesos de auditoría homogéneos y útiles que pueda ser modificada de acuerdo a las condiciones especiales en que se ejecute e incluso a los cambios tecnológicos. El auditor no debe esperar que el modelo sustituya su experiencia, su intuición y el análisis de las condiciones especiales de cada sitio auditado, por el contrario el modelo se basa en ellos y solo establece un patrón a seguir para obtener resultados acordes a las necesidades de una organización como la Universidad de Los Andes.

2.4 Descripción de los módulos que conforman el modelo

Como hemos definido anteriormente el modelo propuesto está constituido por 4 módulos. Estos son:

A) Definición de las condiciones
B) Definición de las características técnicas
C) Pruebas de Penetración
D) Revisiones

En esta sección definiremos más en detalle los objetivos de cada módulo, el por qué de su selección, así como de las secciones que lo componen.

2.4.2 Módulo: Definición de las condiciones

El objetivo principal de este módulo es definir los detalles del proceso de auditoría a realizar. Este módulo debe siempre realizarse antes del inicio del proceso de auditoría. Cualquier proceso de auditoría debe comenzar definiendo los detalles que constituyen la salida de este módulo. Al ejecutarlo los responsables de auditoría deben ser capaces de definir:

- Objetivos Generales.
- Alcance.
- Necesidades de información para el inicio de la auditoría.
- Conformación del equipo auditor.
- Requerimientos técnicos del equipo auditor.
- Conformación de la contraparte.
- Cronograma de entregas.
- Requisitos de confidencialidad y retorno de información.
- Condiciones de garantía de los resultados.

Definiremos cada una de esas unidades de información al momento de presentar las reglas que producen a cada una en este módulo.

Esta etapa del proceso de auditoría es posiblemente más gerencial que técnica, y es una de las más importantes. Una auditoría de calidad debe enfocarse en criterios claramente definidos y documentados. Según [HMATS] La auditoría solamente se lleva a cabo si, luego de consultar con el cliente, es opinión del auditor líder que :

- Existe información suficiente y apropiada sobre el tema a auditar
- Existen recursos adecuados que respalden y avalen el proceso de la auditoría.

- Existe una cooperación adecuada por parte del auditado.

Para asegurar la objetividad del proceso de auditoría, sus resultados y cualquier conclusión, los miembros del equipo auditor deben ser independientes de las actividades que auditan, deben ser objetivos, y libres de tendencia o conflicto de intereses durante el proceso. [KLHCA]

Además de la definición de metas, objetivos y el alcance uno de los elementos fundamentales que debe salir de este módulo es la conformación del equipo auditor. Dicho equipo debe ser una combinación adecuada de conocimientos técnicos y experiencia como auditor.

2.4.3 Módulo definición de las características técnicas

El objetivo fundamental de este módulo es definir los detalles de la red que será auditada. El mismo debe realizarse ANTES del inicio de las pruebas y revisiones y DESPUÉS de haber definido las características del proceso de auditoría.

Como resultado de la ejecución del módulo, el equipo auditor debe obtener el inventario completo de la arquitectura que deberá ser auditada, incluyendo:

- Espacio de direcciones
- Mecanismos de distribución de direcciones
- Descripción de conexiones
- Dispositivos de red
- Servidores
- Estaciones clientes
- Dispositivos de Seguridad

Este módulo está compuesto por las siguientes secciones[7]:

A) Caracterizar el rango de IP que utiliza la organización
B) Definir la forma en que se asignan las direcciones IP de la organización
C) Definir los dispositivos de red
D) Definir estructura de dominios
E) Caracterizar los enlaces de comunicaciones existentes
F) Caracterizar cada equipo servidor
G) Caracterizar equipos clientes

Cada sección de las mencionadas anteriormente está constituida por varias pruebas. Luego de ejecutar el módulo, el equipo auditor debería tener una visión muy completa, desde el punto de vista técnico, del sitio a auditar. Muchas veces este conocimiento permite validar o incluso desechar información ofrecida por el auditado en el primer módulo. Tal fue el caso del escenario en que se probó el modelo y

[7] Si el lector utiliza una versión digital de este documento podrá utilizar los hiperenlaces establecidos en cada sección para revisar directamente el código correspondiente en el modelo que se encuentra en el siguiente capítulo.

que será descrito más adelante en este documento.

La participación del auditor en este módulo es activa. Los resultados se obtienen realizando pruebas, algunas de ellas incluso intrusivas, en la red del auditado.

El módulo pudiese ser dividido en 2 grandes grupos de reglas. Las primeras tienen como objetivo la caracterización de los rangos de direcciones IP (Ipv4 ó Ipv6) que utiliza el sitio auditado, incluyendo direcciones virtuales, direcciones privadas y direcciones fijas, así como el mecanismo por el cual estas direcciones son asignadas. El segundo grupo de reglas están pensadas para caracterizar técnicamente los equipos que serán auditados, incluyendo equipos de comunicaciones, servidores, estaciones clientes y cualquier dispositivo capaz de manejar información y que se encuentre dentro de los objetivos de la auditoría.

Como resultado de este proceso pudiese ser necesario reevaluar los resultados del primer módulo, al descubrir el equipo auditor condiciones técnicas no declaradas que cambien el alcance u otros elementos de salida del módulo 1.

2.4.4 Módulo Pruebas de Penetración

Este módulo define las acciones a llevar a cabo para realizar pruebas de penetración externas e internas sobre la arquitectura bajo estudio. Antes de continuar es necesario definir que se entiende por Pruebas de Penetración. La siguiente definición[SANS] es muy completa:

Las pruebas de penetración o "ethical hacking", son un conjunto de metodologías y técnicas para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso a cualquier entorno informático de un intruso potencial desde los diferentes puntos de exposición que existan, tanto internos como externos.

Para la ejecución de las pruebas de penetración deben seguirse las siguientes reglas [MSSPT]:

- La prueba de penetración de seguridad se inicia recopilando toda la posible información relativa a la infraestructura y las aplicaciones involucradas. Este paso es fundamental, ya que sin un conocimiento sólido de la tecnología subyacente, podrían omitirse algunas pruebas durante la fase de pruebas.
- Los auditores deberían intentar explotar todas las vulnerabilidades descubiertas. Aún cuando la explotación falle, el auditor obtendría un mayor conocimiento del riesgo de la vulnerabilidad.
- Cualquier información obtenida verificando las vulnerabilidades (por ejemplo, errores de programación, obtención de código fuente, u otro descubrimiento de información interna) debería utilizarse para volver a evaluar el conocimiento general de la aplicación y como se ejecuta ésta.
- Si, en cualquier punto durante la prueba, se detecta una vulnerabilidad que pueda llevar al compromiso del objetivo o pueda mostrar información crítica para la organización auditada,

debe ponerse en contacto inmediatamente con la contraparte auditada y hacer que tome conciencia del riesgo involucrado.

Es importante entender la posición del auditor durante la ejecución de las pruebas de penetración. El auditor debe comportarse como un atacante que busca encontrar sitios por donde penetrar y luego comprometer la infraestructura de IT de la organización auditada. En ese proceso obtener la mayor cantidad posible de información de la organización no es un proceso repetitivo (tomando en cuenta los módulos anteriormente ejecutados del modelo). Aquí el objetivo y los métodos son diferentes. Se busca encontrar aquello que un intruso pudiese llegar a conocer de la organización. No debe olvidarse que el conocimiento detallado de la organización es uno de los primeros elementos que procurará un atacante. Veamos un ejemplo. El atacante sabe que la organización a la que desea atacar tiene un servidor WEB pero, ¿Que versión posee del demonio web? ¿Se permite que los usuarios coloquen sus propias páginas? ¿ Qué sistema operativo está corriendo el servidor? [SILHTCP][SHENS][MSSPT][FORUG] Estos son algunos de los elementos que el atacante desearía conocer antes de comenzar su ataque. Otro ejemplo fue obtenido de la ejecución de las pruebas del modelo: durante el proceso de auditoría se descubrió el rango de direcciones privadas del sitio auditado, como consecuencias de errores en la configuración de servicio DNS. Esta información no había sido suministrada al iniciar el proceso de auditoría y permitió acceder de manera más sencilla a información confidencial del sitio auditado.

Una vez conocida, siguiendo los métodos de un atacante, la mayor cantidad de información de la empresa auditada, el siguiente paso será verificar las vulnerabilidades y errores de las aplicaciones que se identifiquen. En este proceso es muy importante descartar falsos positivos y negativos[8].

La salida del módulo debe ser un inventario completo de las vulnerabilidades (incluyendo el acceso a información de la organización, los sistemas, etc...) y errores encontrados con sus correspondientes niveles de ponderación y un glosario de las evidencias que soporten los hallazgos realizados.

Este módulo está compuesto por las siguientes secciones:

A) Definir arquitectura de IT sin conocimiento
B) Generar condiciones de DoS[9]
C) Ejecutar Pruebas contra Firewalls
D) Identificar vulnerabilidades en Servidores WEB
E) Identificar errores básicos de configuración en servidores SMTP
F) Identificar errores básicos de configuración en ambientes inalámbricos
G) Identificar errores de la configuración básica de servidores Unix ó GNU/Linux
H) Fisgonear información sensible en la red
I) Identificar errores básicos de la configuración de servidores Windows

[8] Situaciones que parecen errores pero no lo son y viceversa, situaciones que parecen normales y que en realidad esconden errores o vulnerabilidades serias.

[9] Negación de Servicios

Dependiendo de las características técnicas pudiese no aplicar todas las secciones. La selección de los objetivos ha sido realizada tomando en cuenta los servicios de RedULA y pudiesen servir para la mayoría de las organizaciones.

2.4.5 Módulo Revisiones de las Configuraciones

Aunque la realización de las pruebas de penetración es un elemento muy importante y da una visión de lo que un intruso pudiese hacer, no es suficiente. Existen otras muchas condiciones de riesgo que no serán encontradas durante un proceso de intrusión y que sin embargo pudiesen acarrear problemas de seguridad. Pongamos un ejemplo: una partición de disco de un servidor con poco espacio, consecuencia de una mala planificación de capacidades, pudiese significar la paralización de un servicio pero difícilmente será encontrada por un intruso. Supongamos que un intruso desea probar el sistema de correo de una organización. Para hacerlo genera correos con direcciones falsas (falso el nombre de usuario, no el dominio). En condiciones normales el sistema reenviará al dominio de destino el mensaje y recibirá un mensaje de que el usuario no existe. Este proceso llevará a aumentar el tamaño de las colas de correo y eventualmente hará colapsar a un sistema mal dimensionado. El atacante posiblemente buscaba otro objetivo pero consiguió la paralización del sistema de correo. Ejemplos de este tipo existen muchos.

Por la razón antes expuesta se hace necesario un tipo de auditoría sistemática, en la que el auditor revisa un grupo de elementos adicionales que están relacionados. Encontrar este tipo de relaciones es el objetivo del módulo más extenso y complejo que incluye el modelo: Las Revisiones.

Por la extensión y complejidad de este módulo haremos una revisión más detallada de cada una de las secciones que lo componen.

Este módulo está compuesto por las siguientes secciones:

A) Revisión de la Seguridad Física
B) Revisión de Servidores UNIX
C) Revisión de Servidores y Estaciones Windows
D) Revisión de Servidores Sendmail
E) Revisión de Servidores Apache
F) Revisión de la infraestructura inalámbrica
G) Revisión del Sistema de Detección de Intrusos
H) Revisión de Dispositivos Firewalls
I) Revisión de las Políticas de Seguridad

La salida del módulo es un inventario completo de las vulnerabilidades detectadas durante el proceso de revisión sistémica así como de las recomendaciones para superar las condiciones encontradas. Tal como con los otros módulos, cada regla o prueba tiene asociado un nivel de ponderación que permitirá al auditor dar un valor cuantitativo final del nivel de seguridad del auditado. A continuación describiremos con más detalles cada una de las secciones que conforman este módulo del modelo.

A. Revisión de la Seguridad Física

El resultado de esta sección es encontrar condiciones que dentro de la infraestructura física, no de IT, pudiese influir en la seguridad de esta última [GPMASF]. Entre las condiciones que se busca verificar se encuentran:

- Los mecanismos de control de acceso físico a las instalaciones que albergan componentes del sistema de IT.
- Que existan mecanismos de respuesta automática ante intrusiones o situaciones anómalas. Ej. aumento de temperatura, fuego, temblores.
- Que existan mecanismos adecuados de protección de respaldos y de los equipos ante amenazas de hurto o destrucción accidental.
- Que existan mecanismos adecuados de control de las condiciones ambientales que pudiesen influir en el funcionamiento de la tecnología, medios de almacenamiento u otros.
- Que existan medidas de contingencia antes riesgos físicos y que estos estén acordes a las condiciones del lugar y que el personal ha sido entrenado y los conoce.
- Que existan fuentes adicionales de suministro eléctrico.
- Que los equipos de suministro eléctrico están adecuadamente dimensionados y protegidos.

B. Revisión de Servidores basados en Unix.

El objetivo de esta sección es encontrar condiciones de riesgo en equipos que utilicen sistemas operativos basados en Unix (incluyendo GNU/Linux) siguiendo a [CEUSC][BAMLSS][GAPUIS][UWUSS]. Entre las condiciones que se busca revisar están las siguientes:

- Verificar Seguridad del Sistema de Archivos
- Verificar los procesos activos, su forma de inicio y la seguridad básica de los mismos
- Verificar la Seguridad de Contraseñas
- Verificar la seguridad del sistema de manejo de usuarios
- Verificar la efectividad y seguridad del sistema de respaldos
- Verificar la efectividad y seguridad del sistema de detección de intrusos
- Verificar la efectividad y seguridad del sistema de bitácoras
- Verificar la efectividad y seguridad del sistema de control de acceso
- Verificar la efectividad y seguridad del sistema de directorios NFS

C. Revisión de Servidores y Estaciones basados en Windows

El objetivo de esta sección es encontrar condiciones de riesgo en equipos que utilicen sistemas operativos de la familia Microsoft Windows[CEWCG][WISCO][SMITSW][MICTHGO]. Entre las condiciones que se busca revisar están las siguientes:

- Verificar la seguridad del sistema control de usuarios y contraseñas
- Verificar los atributos de Active Directory (AD)
- Verificar la existencia de permisología mínima
- Verificar la seguridad de la configuración básica los servicios y las actualizaciones
- Verificar la protección del stack TCPIP
- Verificar la efectividad y seguridad del sistema de auditoría interna
- Verificar la seguridad de la configuración básica de controladores de dominios
- Verificar la efectividad y seguridad de los servidores DNS
- Verificar la seguridad de la configuración básica del servicio Terminal Server (TS)
- Verificar seguridad de la configuración básica de los servidores DHCP
- Verificar seguridad de servidores WINS

D. Revisión de Servidores SMTP basados en Sendmail

El objetivo de esta sección es encontrar condiciones de riesgo en servidores SMTP basados en Sendmail [NGSSO] [SHSSV]. Existen múltiples versiones de programas que ofrecen funciones similares a Sendmail, pero este último sigue siendo el más utilizado, a pesar de que algunos nuevos programas como qmail, postfix y exim lo superan en algunas prestaciones. Sendmail sigue siendo, al momento de escribir este documento, el manejador de correo utilizado por RedULA.

La sección que nos ocupa cubre los siguientes tópicos:

- Verificar que la versión utilizada no contenga errores insuperables
- Verificar las condiciones generales de funcionamiento del servicio
- Verificar la efectividad y seguridad de las técnicas Anti-Relay
- Verificar existencia de servicios de autentificación
- Verificar la efectividad y seguridad de las técnicas de prevención de ataques del tipo DoS

- Verificar la seguridad de otras opciones

E. Revisión de Servidores Apache

Contrario a lo que sucede con Sendmail, Apache [APASF][FORUG] [RISASE] es el servidor de WEB que domina no sólo para sistemas basados en Unix ó GNU Linux sino incluso en el mundo Windows. A pesar de que Microsoft produce su propio servidor web (Internet Information Server) este no tiene las prestaciones desde el punto de vista de seguridad de Apache. Apache es el servidor Web utilizado por RedULA. Por estas razones, Apache ha sido seleccionado como servidor Web para el modelo de auditoría.

Esta sección cubre los siguientes aspectos:

- Verificar la Seguridad de las condiciones generales de la instalación
- Verificar la Seguridad del ambiente de ejecución de CGI
- Verificar la Seguridad del esquema de protección general

F. Revisión de la Infraestructura Inalámbrica

Actualmente el desarrollo inalámbrico es uno de los aspectos que distingue el crecimiento de las redes de datos. RedULA se ha enfrascado en ese camino. Por otro lado, si bien la utilización de tecnologías inalámbricas permite ampliar el desarrollo de las redes de datos y amplía su campo de incidencia, trae consigo un grupo importante de riesgos [FNWSC][CCWSC][SCANS][[FOLVIW]. Por ejemplo una red mal configurada permitiría el acceso desde sitios remotos. En la terminología de seguridad se llama a esas redes “redes dulces”. El centro de la ciudad de Mérida es un ejemplo de lo que hemos mencionado. Varias redes inalámbrica coexisten en este ambiente sin protección por lo que es posible conectarse a muchas de ellas e incluso acceder a los recursos internos de las organizaciones.

Los siguientes aspectos son cubiertos por esta sección:

- Verificar la seguridad del esquema de autentificación y control de acceso
- Verificar la seguridad del sistema DHCP
- Verificar los mecanismos de control de integridad y confidencialidad
- Verificar la Seguridad del entorno

G. Revisión de la Infraestructura de Detección de Intrusos

Uno de los elementos que conforman actualmente cualquier sistema de protección son los detectores de intrusos. Como los programas antivirus, un detector de intrusos busca patrones que puedan ser identificados en estas circunstancias no como virus, sino como intrusiones, tráfico no permitido o fuera de rango, comportamiento anómalo de los sistemas, etc.

Existen varias subdivisiones de los sistemas de detección de intrusos [SILHTCP]. Aquí nos referiremos a las dos más comunes. La división entre ellos se basa en el sitio donde realizan la búsqueda de patrones. Los detectores de intrusos basados en red buscan patrones en el tráfico en tiempo real que circula por la red. Los detectores de intrusos basados en servidores realizan su función buscando en las bitácoras de los sistemas que protegen.

El éxito de un sistema de detección de intrusos se basa en la correcta configuración de los filtros de tráfico. Un filtro muy estricto generará tantas alarmas que será poco utilizable y será difícil encontrar información realmente útil dentro de una gran cantidad de registros de alarmas poco significativas. Lo contrario ocurre si los filtros son muy débiles, en este caso no se registrarán las alarmas necesarias. Otro aspecto es que el detector de intrusos verifique todos los sitios de acceso o servidores.

Esta sección cubre los siguientes aspectos:

- Verificar la configuración básica de seguridad de un Detector de Intrusos Basado en red (NDIS)
- Verificar la seguridad del sistema los Sistemas de Detección de Intrusos basados en host

H. Revisión de Dispositivos Firewalls

Los dispositivos cortafuegos (*firewalls*) son uno de los baluartes de cualquier sistema de seguridad. Muchos son los aspectos que deben tomarse en cuenta para que un dispositivo firewall sea realmente un dispositivo útil [ZWBIF][TCHRFC]. Hemos seleccionados aquellos más importantes y que están directamente relacionados con el cumplimiento de las funciones de seguridad informática para las cuales una organización coloca un dispositivo firewall en su red:

- Verificar efectividad de las reglas de filtrado

- Verificar efectividad de las políticas de mantenimiento de la configuración
- Verificar configuración y seguridad del sistema de bitácoras

I. Revisión de las Políticas de Seguridad Informática

Aunque muchas veces suele subestimarse su importancia, la existencia de Políticas de Seguridad dentro de una organización es uno de los elementos esenciales para que las metas de seguridad informática puedan ser cumplidas adecuadamente.
Existen muchos documentos que tratan sobre como implantar correctamente una política de seguridad organizacional y que elementos debe contener esta. El documento que casi todos los expertos reconocen como la guía fundamental es el ISO 17799 [CRISPMS][ISO17799]. Esta última sesión del modelo está basado en él. El ISO está compuesto por 10 capítulos:

CAP 1 De la Propia Política de Seguridad

CAP 2 Seguridad Organizacional

CAP 3 Clasificación y Control de Activos

CAP 4 Seguridad Personal

CAP 5 Seguridad Física y Ambiental

CAP 6 Gestión de Operaciones y Comunicaciones

CAP 7 Control de Acceso

CAP 8 Desarrollo y Mantenimiento de Sistemas

CAP 9 Gestión de la Continuidad de Negocio

CAP 10 Cumplimiento del Marco Jurídico

De igual manera han sido organizados los aspectos dentro de esta sección del modelo:

- Verificar el cumplimiento de los objetivos del Cap 1 ISO17799
- Verificar el cumplimiento de los objetivos del Cap 2 ISO17799
- Verificar el cumplimiento de los objetivos del Cap. 3, ISO17799
- Verificar el cumplimiento de los objetivos del Cap 4 ISO17799
- Verificar el cumplimiento de los objetivos del Cap. 5 ISO17799
- Verificar el cumplimiento de los objetivos del Cap 6 ISO17799
- Verificar el cumplimiento de los objetivos del Cap 7 ISO17799

- Verificar el cumplimiento de los objetivos del Cap 8 ISO17799
- Verificar el cumplimiento de los objetivos del Cap. 9 ISO17799
- Verificar el cumplimiento de los objetivos del Cap 10 ISO17799

En este capítulo hemos descrito la arquitectura general de nuestro modelo de auditoria que está compuesto por 4 módulos o grupos funcionales. En el capítulo siguiente se desglosan los detalles de cada uno de esos módulos al nivel de secciones y luego de las reglas del cómo proceder en cada sección.

Capítulo 3. Modelo de Auditoría de Seguridad para RedULA

El trabajo de auditoría consiste de la ejecución del procedimiento que se muestra a continuación:

Desarrollo General

PARA "Realizar un proceso de auditoría de seguridad" {
I. *Definición de las condiciones del proceso de auditoría*
II. SI "Se realizó Definición de las condiciones del proceso de auditoría" ENTONCES *Definición inicial de las características técnicas del sistema*
III. SI ¨ Se realizaron I y II Y Es requerido[10]" ENTONCES *Pruebas de Penetración*
IV. SI ¨ Se realizaron I y II Y Es requerido[11]" ENTONCES Revisiones
}

Desde luego, este es el más alto nivel de abstracción del proceso. A continuación, desglosamos los detalles:

[10] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar pruebas de penetración sin conocimiento para la ejecución del proceso de auditoría. Las pruebas de penetración pueden realizadas por separado, sin necesidad de realizar otras pruebas.

[11] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar Revisiones. Por regla general las revisiones son siempre requeridas a no ser que se trate de un ejercicio sólo de Pruebas de Penetración.

Definición inicial de las condiciones del proceso de auditoría

Objetivo de este módulo: Definir los detalles del proceso de auditoría a realizar. Esta sección debe realizarse ANTES del inicio del proceso de auditoría.

Salida : Definición de los detalles del proceso. A saber,

- Objetivos Generales.
- Alcance.
- Necesidades de información para el inicio de la auditoría.
- Conformación del equipo auditor.
- Requerimientos técnicos del equipo auditor.
- Conformación de la contraparte.
- Cronograma de entregas.
- Requisitos de confidencialidad y retorno de información.
- Condiciones de garantía de los resultados.

1. PARA "Definición Inicial de las condiciones del proceso de auditoría"
   1.1 Identificar los objetivos generales del proceso de auditoría
   1.2 Definir el alcance del proceso de auditoría
   1.3 Definir la información que debe ser entregada por el auditado para comenzar el proceso de auditoría
   1.4 De acuerdo a los objetivos de la auditoría, definir conformación del equipo auditor
   1.5 De acuerdo a los objetivos de la auditoría definir los requerimientos técnicos
   1.6 Definir con el auditado los detalles de la conformación del equipo profesionales que acompañará al equipo auditor y los mecanismos de comunicación entre ellos
   1.7 Definir con el auditado el cronograma de entregas
   1.8 Definir con el auditado los requerimientos de confidencialidad, los mecanismos de entrega de información y de retorno de la información entregada al inicio del proceso
   1.9 Definir con el auditado los detalles sobre el proceso de garantía de los resultados una vez concluida la auditoría.

Definición técnica inicial del sistema.

Objetivo de esta sección: Definir los detalles de la red que será auditada. Esta sección debe realizarse ANTES del inicio de las pruebas y revisiones y DESPUES de haber definido las características del proceso de auditoría.

Salida : Inventario completo de la arquitectura que deberá ser auditada, incluyendo:

- Espacio de direcciones
- Mecanismos de distribución de direcciones
- Descripción de conexiones
- Dispositivos de red
- Servidores
- Estaciones clientes
- Dispositivos de Seguridad

DESARROLLO:

PARA " Caracterizar Técnicamente el Sistema a Auditar" {

I. Caracterizar el rango de IP que utiliza la organización
II. Definir la forma en que se asignan las direcciones IP de la organización
III. Definir los dispositivos de red
IV. Definir estructura de dominios
V. Caracterizar los enlaces de comunicaciones existentes
VI. Caracterizar cada equipo servidor
VII. Caracterizar equipos clientes}

1. PARA "Caracterizar del rango IP que utiliza la organización"
   1.1 SI "el rango de direcciones internas es privado " ENTONCES
      1.1.1 PARA "Definir el esquema de numeración de las direcciones IP encontrando:"
         1.1.1.1 Direcciones VIP (Virtual IP) (externas)
         1.1.1.2 Mapas de traducción de direcciones
         1.1.1.3 Rangos de direcciones de salida especificando direcciones que corresponden a cada VIP y al pool de la red.
         1.1.1.4 Forma en que se asignan las direcciones IP (estáticas o por DHCP)
   1.2 SI "el rango de direcciones internas es público " ENTONCES Definir quien

es el proveedor oficial del rango de direcciones y con quienes se comparte (vecinos mas cercanos en ambos sentidos)

2 PARA "Definir la forma en que se asignan direcciones IP para la organización"

2.1 SI "las direcciones son asignadas dinámicamente" ENTONCES Definir cuales son los servidores DHCP

2.1.1.1 Por cada uno encontrar los parámetros de asignación de las direcciones IP estableciendo, como mínimo:

2.1.1.2 Rango de direcciones asignables

2.1.1.3 Asignación estática de direcciones

2.1.1.4 DNS asignados

2.1.1.5 Rutas por omisión

2.1.1.6 Impresoras de red

2.1.1.7 Servidores WINS

2.1.1.8 Servidores de Dominio

2.2 DE LO CONTRARIO Definir el mapa completo de rangos de direcciones asignadas encontrando:

2.2.1 Direcciones[12] asignadas a servidores

2.2.2 Direcciones asignadas a dispositivos de telecomunicaciones

2.2.3 Direcciones asignadas a dispositivos de ofimática

2.2.4 Direcciones asignadas a estaciones clientes y otros dispositivos

2.2.5 Direcciones libres

2.2.6 Mecanismo gerencial de asignación de direcciones (si existe algún protocolo para la asignación)

3 SI " existe un ambiente híbrido[13] ENTONCES Definir para cada ambiente lo establecido en los puntos 1 y 2.

3.1 Establecer el punto de unión de ambos ambientes

3.2 Definir la política de pertenencia a cada ambiente

4 PARA "Definir los dispositivos de red[14] que existen

4.1 Definir Función

4.2 Definir Marca, modelo y fabricante

4.3 Definir Sistema Operativo, versión y parches (si aplica)

4.4 Definir Relación de dependencia con otros dispositivos

[12] A efecto se sencillez se ha colocado sólo el término dirección IP. Se sobre entiende que se refiere también a la máscara IP en cada caso.

[13] Por **híbrido** se entiende cualquier combinación de las establecidas anteriormente. ej. Existen direcciones privadas y públicas, las direcciones se asignan por DHCP y de forma estática"

[14] Routers, VPN Gateways, firewalls, NIDS

4.5 Definir Servicios que ejecutan [15]
4.6 Definir Comunidades SNMP

5 SI "existen dominios[16] ENTONCES
5.1 PARA " Definir estructura de los dominios"
5.1.1 Definir integración de los mismos[17]
5.1.2 Definir estructura jerárquica de los mismos y la función de cada nivel de la estructura
5.1.3 Definir responsables de cada dominio
5.1.4 Definir funciones de cada dominio
5.1.5 Definir la delegación de dominios

6 PARA " Caracterizar los enlaces de comunicaciones existentes"
6.1 Definir Redes que interconectan
6.2 Definir Dispositivos involucrados
6.3 Definir Ancho de banda
6.4 Definir Tecnología
6.5 Definir Características de seguridad que se utilizan[18]
6.6 Definir Política de uso del medio[19]
6.7 Definir Proveedor de servicios

7 PARA " Caracterizar cada equipo servidor
7.1 Definir Modelo
7.2 Definir Sistema Operativo
7.3 Definir Versión
7.4 Definir Servicios que se ejecutan
7.5 Definir Versión de los servicios
7.6 Definir Nivel de actualizaciones
7.7 Definir Localización física
7.8 Definir Responsable
7.9 Definir Dispositivos conectados
7.10 Definir Arquitectura (cantidad de memoria, tamaño de disco)
7.11 Definir Sistemas de protección eléctrica
7.12 Definir Sistemas Antivirus
7.13 Definir Sistemas de Seguridad

8 PARA " Caracterizar los equipos clientes[20]"

[15] Por Servicios se entiende: HTTP, HTTPS, SMTP, SNMP, etc...
[16] LDAP, AD, DNS, NIS
[17] Se refiere a la integración operativa , por ejemplo entre DNS y LDAP ó AD
[18] Ej: VPN, Cifrado simple de la información, autentificación de los bordes de la conexión
[19] Control de Protocolos, enlaces P2P, control de ancho de banda por períodos de tiempo, etc..
[20] En este caso se estima definir la arquitectura típica mas general

8.1 Definir Modelo
8.2 Definir Sistema Operativo
8.3 Definir Versión
8.4 Definir Servicios que se ejecutan
8.5 Definir Versión de los servicios
8.6 Definir Nivel de actualizaciones
8.7 Definir Localización física
8.8 Definir Responsable
8.9 Definir Dispositivos conectados
8.10 Definir Arquitectura (cantidad de memoria, tamaño de disco)
8.11 Definir Sistemas de protección eléctrica
8.12 Definir Sistemas Antivirus utilizados
8.13 Definir Sistemas de Seguridad utilizados

Pruebas de penetración

DESARROLLO:

PARA "Realizar Pruebas de Penetración" {

I. Definir arquitectura de IT sin conocimiento
II. Generar condiciones de DoS[21]
III. Ejecutar Pruebas contra Firewalls
IV. Identificar vulnerabilidades en Servidores WEB
V. Identificar errores básicos de configuración en servidores SMTP
VI. Identificar errores básicos de configuración en ambientes inalámbricos
VII. Identificar errores de la configuración básica de servidores Unix ó GNU/Linux
VIII. Fisgonear información sensible en la red
IX. Identificar errores básicos de la configuración de servidores Windows }

1 PARA "Definir arquitectura sin conocimiento[22] desde la Internet[23]"

1.1 Utilizando herramientas de búsqueda automatizada rastrear puntos de conexión de la red con el exterior, servidores visibles desde el exterior, rango de direcciones disponibles, anuncios de DNS.

1.1.1 SI "es posible identificar "Puntos de conexión de la red con el exterior" ENTONCES Recomendar revisar las políticas de control de acceso y transferencia de información vía ICPM, SNMP, etc...

1.1.2 SI "es posible identificar "Servidores visibles desde el exterior"" ENTONCES

1.1.2.1 PARA "caracterizar servidores visibles desde el exterior"

1.1.2.1.1 Definir Versión de los servicios visibles desde el exterior.

1.1.2.1.2 Definir Servicios que se ofrecen.

1.1.2.1.3 Definir Información de la organización obtenible a partir de los servicios que se ofrecen

1.1.2.1.4 Buscar servicios que no debiesen ser expuestos al exterior.

1.1.3 SI "es posible identificar "Rango de direcciones disponibles" ENTONCES Recomendar revisar las políticas de control de acceso y transferencia de información vía ICPM, SNMP, etc..."

1.1.4 SI "es posible identificar anuncios de DNS" ENTONCES Definir zonas

1.1.4.1 SI "se logra hacer transferencias de zonas satisfactorias" ENTONCES Recomendar revisar la seguridad de los servicios DNS.

[21] Negación de Servicios

[22] Se refiere a la realización de las pruebas sin conocimientos especiales de la arquitectura del sitio auditado más allá de que sea posible obtener de la información pública de la organización.

[23] Se utiliza el término genérico Internet para referirse a cualquier red fuera del perímetro de la red auditada.

1.1.4.2 SI "se pueden hacer hacer solicitudes de direcciones que no deberían estar expuestas[24]" ENTONCES Recomendar revisar las políticas de inscripción en DNS.

1.1.4.3 Utilizando la información recabada del DNS utilizar una herramienta de enumeración para obtener el listado de servidores y hacerla coincidir con los servidores identificados en el paso 1.1.2

1.1.5 Ejecutar un rastreo completo del rango de direcciones definidas anteriormente utilizando solo SNMP[25]

1.1.5.1 SI "se logran identificar equipos utilizando SNMP" ENTONCES Recomendar revisión de los parámetros de configuración de los equipos identificados

1.1.5.1.1 Recomendar revisión de las políticas de filtrado de información de la red.

1.1.5.1.2 Tratar de identificar la función de cada dispositivo.

1.2 Utilizando la información de obtenida en el paso 1 tratar de armar un mapa lo más detallado posible de la red a auditar.

1.3 Utilizar varias herramientas de búsqueda de vulnerabilidades y hacer un listado completo de las vulnerabilidades detectadas, eliminando aquellas que puedan ser determinadas como falsos positivos.

2 PARA " Generar condiciones de negación de servicios[26]"

2.1 SI "existen servidores WEB" ENTONCES Realizar pruebas de stress aumentando el nivel de carga en hacia el servidor para encontrar el punto de inflexión de rendimiento del servidor contra carga generada[27].

2.2 SI "existen servidores de CORREO" ENTONCES Realizar pruebas de stress aumentando el nivel de carga en hacia el servidor para encontrar el punto de inflexión de rendimiento del servidor contra carga generada[28].

2.3 Sobre los equipos de COMUNICACIONES comenzar a generar tráfico hacia ellos[29] variando el tipo de tráfico, el tamaño de los paquetes y la velocidad de transferencia.

2.4 Generar tráfico hacía el broadcast[30] de la red.

2.4.1 SI "se reciben mensajes de respuesta" ENTONCES Recomendar revisar las políticas de filtrado de tráfico en el router de borde especialmente la prohibición de envío/recepción de paquetes enviados/dirigidos desde/hacia el broadcast de las redes detrás del router.

2.5 Generar tráfico SYN hacia objetivos seleccionados en la red bajo prueba.

2.5.1 SI se logra generar condiciones altas de tráfico que comprometan el funcionamiento del sistema ENTONCES SI "El nivel crítico se logrado con bajo nivel de tráfico" ENTONCES

[24] Ej. Estaciones clientes, direcciones privadas, routers, firewalls, equipos de comunicaciones

[25] Utilizar las comunidades por omisión y aquellos nombres que pudiesen estar relacionados con la organización y su entorno.

[26] Estas pruebas deberán ser realizadas desde el exterior e interior de la red. Cuando las pruebas se realicen desde el exterior y tengan éxito habrá que Recomendar la revisión de las políticas de filtrado y control de acceso.

[27] Luego estos valores deberá ser comparados con las dimensiones de la población esperada que usen el servicio

[28] Luego estos valores deberá ser comparados con las dimensiones de la población esperada que usen el servicio

[29] Debe ser tráfico que pueda ser medido en el punto de origen. ICMP es una excelente opción.

[30] Esta prueba deberá ser realizada con sumo cuidado pues puede provocar la "caída" del sistema auditor.

Recomendar:

- Ampliar el tamaño de las cola de conexión en los dispositivos afectados.
- Disminuir el período de establecimiento de la conexión .

2.5.2 Buscar evidencias de detección del tráfico anormal.

2.5.2.1 SI " No se encuentran evidencias de que el tráfico haya sido detectado" ENTONCES Recomendar implantación de sistemas de detección de intrusos basados en red. (NIDS). Y recomendar aplicar las actualizaciones necesarias para parar y detectar Inundación SYN.

2.6 Identificar los servidores DNS e intentar introducir datos falsos en los mapas durante las transferencias de zona[31].

2.6.1 SI "se logra falsear información" ENTONCES Recomendar revisar la políticas de seguridad del servidor DNS e instalar las actualiza los servicios DNS.

2.7 Utilizar un programa SMBdie[32] para generar condiciones de caída a los servidores WindowsX.

2.7.1 Si "la prueba tiene éxito[33]" ENTONCES Recomendar actualizar los servidores afectados y la política de filtrado NETBIOS desde el exterior.

2.8 SI "existen sistemas identificados como WINDOWS NT" ENTONCES Generar tráfico mal formado desde direcciones escogidas de forma aleatoria y cambiante y verificar niveles de CPU de los sistemas atacados. SI " la prueba tiene éxito[34]" ENTONCES Recomendar evaluar la necesidad de dimensionar adecuadamente las capacidades de procesamiento de los equipos sometidos a prueba.

2.9 Identificar servidores WEB que realicen autentificación de entrada. Introducir contraseñas largas[35]. SI " la prueba tiene éxito[36]" ENTONCES Recomendar rediseñar las rutinas de autentificación para que detecten esta condición.

3 PARA "Ejecutar pruebas contra los firewalls"

3.1 SI "existen filtros de paquetes " ENTONCES "Identificar identificar las reglas de filtrado" SI "la prueba tiene éxito[37]" ENTONCES Identificar reglas que afecten directamente la capacidad del firewall de dar información sobre si mismo.

3.1.1.1 Identificar reglas que limiten el acceso a servicios internos.

3.1.1.2 Identificar faltas en la reglas de filtrado, especialmente determinando la existencia de reglas tolerantes.

3.1.1.3 Recomendar el bloqueo de paquetes con ICMP TTL EXPIRED

3.2 Verificar la posibilidad de "atravesar" el firewall utilizando paquetes ICMP ECHO, ECHO REPLAY y UDP. SI "la prueba tiene éxito" ENTONCES

- Alertar sobre la posibilidad de pasar el firewall encapsulando tráfico en esos protocolos.

[31] Utilizando una técnica de "hombre en medio" entre los servidores DNS.

[32] Microsoft Security Bulletin MS02-045

[33] Éxito para esta prueba significa que los servidores se caen

[34] Éxito para esta prueba significa que los servidores aumentan los niveles de carga de CPU

[35] 40000 caracteres o más.

[36] Éxito para esta prueba significa que los servidores aumentan los niveles de carga de CPU

[37] Éxito en esta prueba significa que se puedan identificar que servicios está siendo filtrados por el firewall.

- Alertar sobre el tipo de información que puede obtenerse de estos protocolos. Recomendar el filtrado de los tipos de servicios (ICMP) y puertos (UDP) no necesarios.
- Recomendar el bloqueo o desvío de tráfico como el señalado.

3.3 Generar tráfico segmentado hacia dentro de la red y verificar la política de control de fragmentos del firewall.

3.3.1 SI "el firewall detiene sólo el primer paquete" ENTONCES Alertar sobre la posibilidad de pasar tráfico hacia la red utilizando el resto de los fragmentos.

3.3.2 SI "el firewall losdetiene todos" ENTONCES Alertar sobre la posibilidad de ataques de DoS.

3.4 SI "existen servidores proxy" ENTONCES Verificar el acceso anónimo desde el exterior.

4 PARA "Identificar vulnerabilidades en Servidores WEB"

4.1 Utilizar una herramienta especializada para la búsqueda de vulnerabilidades en servidores WEB.

4.2 SI "existen servidores que autentifiquen a los usuarios" ENTONCES Ejecutar pruebas de fuerza bruta y diccionarios para encontrar claves débiles

4.2.1 Obtener el archivo .htaccess (o el equivalente) utilizar una herramienta[38] para romper las contraseñas almacenadas. Si "la prueba tiene éxito" ENTONCES Recomendar mejora de la política de contraseñas.

4.2.1.1 Seleccionar las contraseñas encontradas y penetrar el sistema.

4.3 PARA " Identificar vulnerabilidades en servidores que utilicen IIS"

4.3.1 Explorar la posibilidad de utilizar código ASP de ejemplo[39] para explorar código fuente de otras aplicaciones. SI "la prueba tiene éxito"[40] ENTONCES Recomendar la de-instalación de los códigos de ejemplo asp e instalar los parches del fabricante.

4.3.2 SI "es posible descargar archivos utilizando la cadena ::DATA" ENTONCES Recomendar actualización de IIS.

4.3.3 Enviar secuencia GET solicitando un archivo al servidor terminada por la sentencia traslade:f. SI "es posible obtener un archivo" ENTONCES Recomendar actualización del servidor web.

4.3.3.1 Verificar si dentro de los archivos obtenidos se encuentran claves u otra información relevante . SI "la prueba tiene éxito" ENTONCES Recomendar rediseño de la aplicación para ocultar este tipo de información.

4.3.4 SI "existen formularios sin sistemas de autentificación capcha" ENTONCES Recomendar el rediseño de todos los formularios para incluir este tipo de elementos.

4.3.5 Explorar la posibilidad de utilizar aplicaciones tipo ISSHack para ejecutar comandos remotos a través del servidor.[41] SI "la prueba tiene éxito[42]" ENTONCES Recomendar actualizar el servidor.

4.4 Utilizar un motor de búsquedas para de sitos de administración incorrectamente indexados.[43] SI

[38] Ej: Jhon the Ripper

[39] showcode.asp y codebrws.asp

[40] Utilizando estas aplicaciones se puede explorar el código de otras aplicaciones como boot.init

[41] http://www.technotronics.com

[42] Éxito en esta prueba significa que se pueda instalar un programa en el servidor .

[43] ej. /admin, /password,/password.txt, type=hidden name=price, etc...

"la prueba tiene éxito[44]" ENTONCES Recomendar revisar completamente la estructura del sitio WEB comprometido.

4.5 Generar procesos de inyección SQL contra el servidor[45]. SI "la prueba tiene éxito[46]" ENTONCES Recomendar rediseñar los mecanismos de validación de entrada siguiendo reglas más estrictas.

5 PARA "Identificar errores básicos de configuración en servidores SMTP"

5.1 Conectándose al puerto 25 tratar de:

5.1.1 Pasar sin helo. SI "la prueba tiene éxito" ENTONCES Recomendar reconfigurar el servidor de correo para que solicite siempre el comando helo.

5.1.2 Enviar comando helo sin nombre de máquina. SI "la prueba tiene éxito" ENTONCES Recomendar reconfigurar el servidor de correo para que solicite siempre el nombre de la máquina

5.1.3 Enviar comando MAIL FROM: con un nombre aleatorio sin dominio. SI "la prueba tiene éxito" ENTONCES Recomendar reconfigurar el servidor de correo para que solicite el dominio

5.1.4 Enviar comando MAIL FROM: utilizando un dominio que no exista. SI "la prueba tiene éxito" ENTONCES Recomendar reconfigurar el servidor de correo para que verifique siempre la resolución de nombres del dominio de origen.

5.1.5 Enviar comando RCPT TO: utilizando un usuario no local. SI "la prueba tiene éxito" ENTONCES Recomendar reconfigurar el servidor de correo para que impida ser utilizado como RELAY.

5.2 Generar correos hacia el interior de la organización con attach normalmente no aceptados[47] SI "la prueba tiene éxito" ENTONCES Recomendar reconfigurar el servidor de correo para que filtre los archivos adjuntos.

5.3 Generar correos hacia el interior de la organización con attach normalmente no aceptados[48] SI "la prueba tiene éxito" ENTONCES Recomendar reconfigurar el servidor de correo para que filtre los archivos adjuntos.

5.4 Generar correos hacia el interior de la organización desde direcciones reconocidas como generadores de SPAM. SI "la prueba tiene éxito[49]" ENTONCES Recomendar reconfigurar el servidor de correo para que filtre las fuentes reconocidas como SPAM.

6 PARA " Identificar errores básicos de configuración de ambientes inalámbricos"

6.1 Utilizar herramientas de "war-driving" para identificar los puntos de acceso inalámbricos, modelos, direcciones IP, tipos de cifrado. SI "se detectan que existe control por MAC" ENTONCES clonar la dirección MAC de las estación cliente y conectarse a la red. Recomendar que el filtrado MAC no es una solución satisfactoria de control de acceso.

[44] Éxito en esta prueba significa que se pueda encontrar sitios como los señalados en 24 .

[45] Utilizar una herramienta automatizada como Wpoison.

[46] Éxito en esta prueba significa se encuentren vulnerabilidades que permitan efectuar la inyección SQL .

[47] ej. Programas ejecutables, archivos infectados con virus, etc...

[48] Para este caso de tamaños variables y siempre incremental

[49] Tener éxito en esta prueba significa que los correos lleguen a los usuarios sin marcas de SPAM hechas por el servidor.

6.2 SI "se utiliza WEP como elemento de cifrado" ENTONCES utilizar alguna herramienta para romper las contraseñas. SI "la prueba tiene éxito[50]" ENTONCES. SI "el tamaño de las claves no es máximo" ENTONCES Recomendar aumentar tamaño de las claves DE LO CONTRARIO Recomendar cambiar el protocolo de cifrado utilizado.

6.3 Utilizar herramientas[51] para suplantar e inyectar tramas completas generando suficiente tráfico para bajar el rendimiento de la red[52]. SI "la prueba tiene éxito[53]" ENTONCES Recomendar instalar mecanismos de control de tráfico.

7 PARA "Identificar errores de la configuración básica de servidores UNIX ó GNU/Linux"

7.1 Ejecutar pruebas de fuerza bruta[54] para encontrar contraseñas débiles utilizadas en los servicios disponibles. SI "la prueba tiene éxito[55]" ENTONCES Recomendar redefinir la política de contraseñas y de control de intentos.

7.2 Verificar si pueden establecerse sesiones de canal trasero. SI "la prueba tiene éxito[56]" ENTONCES:

- Recomendar cerrar en ambos sentidos las conexiones para impedir conexiones que se originen desde el servidor(es).
- SI "existen servicios X" Recomendar eliminar los servicios X del servidor(es)
- Recomendar la revisión de los permisos de los comandos utilizados por el servicio que se utilizó para establecer el canal trasero.

7.3 Utilizar una herramienta de rastreo de puertos para buscar puertos altos asociados a servicios RPC. SI "la prueba tiene éxito[57]" ENTONCES Recomendar desactivar todos los servicios RPC no necesarios

7.4 Utilizar una herramienta de búsqueda de vulnerabilidades para encontrar errores explotables asociados a RPC.

7.5 SI " existe un servicio FTP anónimo" ENTONCES tratar de ejecutar "site exec" como usuario anónimo. SI "la prueba tiene éxito[58]" ENTONCES Recomendar Actualizar la versión del demonio FTP que se utiliza.

7.6 Buscar exportaciones de subdirectorios con permisología incorrecta. SI "la prueba tiene éxito[59]"

---

[50] Tener éxito en esta prueba significa que se logran obtener las claves de cifrado utilizadas. Esta prueba puede implicar, en función del nivel de tráfico en la red, mucho tiempo de recolección de datos.

[51] Air-Jack es una de ellas.

[52] Contra este tipo de ataque no hay solución efectiva

[53] Que se logra introducir tráfico en la red hasta hacerla colapsar

[54] Esta prueba es altamente intrusiva y puede provocar la caída del sistema, el bloqueo de cuentas y el condiciones de carga elevada en la red y los servicios.

[55] Tener éxito en esta prueba significa que se logran obtener las claves de acceso utilizadas. Esta prueba puede implicar, en función del nivel de tráfico en la red, mucho tiempo de recolección de datos.

[56] Tener éxito en esta prueba significa que se logran establecer sesiones "back end" o de canal trasero debido a errores de configuración del sistema de filtrado.

[57] Tener éxito en esta prueba significa que se logran obtener las claves de cifrado utilizadas. Esta prueba puede implicar, en función del nivel de tráfico en la red, mucho tiempo de recolección de datos.

[58] Tener éxito en esta prueba significa que se logra ejecutar comandos de manera anónima en el servidor FTP. Posiblemente se logre escalada de privilegios.

[59] Tener éxito en esta prueba significa que se logran montar subdirectorios vía NFS incorrectamente permisados.

ENTONCES Recomendar revisar la política de exportación.

7.6.1 SI "el montaje se realizó desde el exterior" ENTONCES Recomendar modificar la forma de exportación para inhabilitar exportaciones simples hacia el exterior de la red y revisar la política de filtrado.

7.7 SI "existen servidores con servicios X habilitados" ENTONCES hacer un rastreo de servidores con xhost+ habilitado.

7.7.1 SI "la prueba tiene éxito[60]" ENTONCES Recomendar desactivar todos los servicios X en los servidores.

7.8 SI "existen servidores DNS" ENTONCES ejecutar herramientas de búsquedas de vulnerabilidades de DNS para encontrar situaciones críticas.

7.8.1 SI "la prueba tiene éxito[61]" ENTONCES Recomendar reparar condiciones de riesgo encontradas.

7.9 SI "existen servidores SSH" ENTONCES ejecutar herramientas de búsquedas de vulnerabilidades de SSH para encontrar situaciones críticas.

7.9.1 SI "la prueba tiene éxito[62]" ENTONCES Recomendar reparar condiciones de riesgo encontradas.

7.10 SI "existen servidores APACHE" ENTONCES ejecutar herramientas de búsquedas de vulnerabilidades de APACHE para encontrar situaciones críticas.

7.10.1 SI "la prueba tiene éxito[63]" ENTONCES Recomendar reparar condiciones de riesgo encontradas

7.11 SI "existen servidores en modo promiscuo" ENTONCES Recomendar que no se utilicen programas "sniffers" en servidores.

8 PARA "Fisgonear información sensible de la red"

8.1 Instalar un equipo con programas sniffers para capturar información de la red[64].

8.2 Seleccionar paquetes que pudiese contener información sensible de usuarios

8.2.1 SI "8.2 ha tenido éxito[65]" ENTONCES Recomendar revisar la forma en que se transfiere información clasificada por la red.

9 PARA " Identificar errores básicos de configuración en servidores Windows"

9.1 Utilizar una herramienta de acceso directo para buscar usuarios sin contraseñas. SI "la prueba tiene éxito[66]" ENTONCES Recomendar redefinir la política de contraseñas y de control de intentos.

---

60 Tener éxito en esta prueba significa que se logran obtener servidores con la opción xhost+ habilitada.

61 Tener éxito en esta prueba significa que se encuentran vulnerabilidades explotables del servicio DNS

62 Tener éxito en esta prueba significa que se encuentran vulnerabilidades explotables del servicio SSH

63 Tener éxito en esta prueba significa que se encuentran vulnerabilidades explotables del servicio HTTP manejado por APACHE

64 Buscar información como contraseñas, transferencias de zona DNS, datos sin cifrar,etc...

65 Tener éxito en esta prueba significa que se pueden capturar paquetes de información identificables y con datos sensibles.

66 Tener éxito en esta prueba significa que se logran obtener las claves de acceso utilizadas. Esta prueba puede implicar, en función del nivel de tráfico en la red, mucho tiempo de recolección de datos.

9.2 Utilizar herramientas especializadas para probar la política de bloqueo de cuentas por intentos no satisfactorios de acceso.

9.3 SI "de 9.1-9.2 se ha realizado desde el exterior de la organización" ENTONCES proponer revisar la política de filtrado para impedir el paso de protocolos de SMB y NetBIOS hacia el exterior de la red.

9.4 Instalar un programa sniffer especializado en contraseñas.

9.4.1 Capturar contraseñas (hash)y someterlas a un esfuerzo de fuerza bruta. SI "la prueba ha tenido éxito " ENTONCES Recomendar revisar y ajustar las políticas de contraseñas.

9.4.1.1 SI " la prueba ha tenido éxito y se ha realizado sobre WINDOWS 2000,XP ó 2003" ENTONCES Recomendar deshabilitar el uso de LM".

9.5 SI "existe IIS" ENTONCES Realizar una solicitud utilizando la extensión +.htr. SI "la prueba tiene éxito[67]" ENTONCES Recomendar redefinir la política de contraseñas y de control de intentos.

9.5.1 SI "se encuentra datos sensibles" en los archivos descargados ENTONCES "Recomendar revisar los archivos para eliminar de ellos información confidencial"

9.5.2 Utilizar una herramienta de búsqueda de vulnerabilidades para encontrar situaciones erróneas en la instalación de IIS.

9.5.3 SI "la prueba tiene éxito[68]" ENTONCES Recomendar reparar condiciones de riesgo encontradas.

9.5.4 Utilizar una herramienta[69] que permita escalar privilegios.

9.5.5 SI "la prueba tiene éxito" ENTONCES Recomendar actualizar el servidor IIS.

9.5.6 Utilizar una herramienta[70] que permita generar condiciones de buffer overflow.

9.5.7 SI "la prueba tiene éxito" ENTONCES Recomendar actualizar el servidor IIS y desactivar los archivos de extensión ISAPI no utilizados.

9.5.8 SI "se ha logrado capturar contraseñas de usuarios" ENTONCES Realizar una conexión local utilizando la cuenta comprometida y ejecutar programas[71] para la escalada de privilegios. Escalar una cuenta con privilegios administrador.

9.5.9 SI "la prueba tiene éxito[72]" ENTONCES Recomendar instalar los parches correspondientes.

9.5.9.1 Utilizar una herramienta[73] para obtener los hash de las contraseñas y utilizar una herramienta de rompimiento de claves para obtener claves del sistema. SI "se logran obtener las claves" Recomendar mejoras en la política de asignación de contraseñas.

9.5.9.2 Utilizar una herramienta[74] para acceder a los valores guardados en LSA Secret. SI " se logran obtener claves" ENTONCES Recomendar actualizar el Sistema Operativo.

[67] Tener éxito en esta prueba significa que se logra obtener el código fuente de los archivos asp solicitados

[68] Tener éxito en esta prueba significa que se encuentran vulnerabilidades explotables del servicio IIS.

[69] Ej: ispc

[70] Ej: jill

[71] Ej: hk, pipeupadmin

[72] Tener éxito en esta prueba significa que se pueda escalar los privilegios del usuario seleccionado dentro del sistema.

[73] Ej:pwdump2 ó pwdump3e

[74] Ej: LSADump2

9.5.10 Utilizar una herramienta de acceso remoto para abrir una interfaz de comando en los servidores bajo estudio.

9.5.10.1 SI "la prueba tiene éxito" ENTONCES Recomendar revisar la política de filtrado y servicios activos.

9.5.10.1.1 Instalar una herramienta[75] en los servidores bajo estudio para acceso de sesiones gráficas. Recomendar revisar la política de filtrado y servicios activos.

[75] Ej: VNC, PCAnyWhere, etc.

Revisiones de las configuraciones

I. PARA "Realizar Revisiones"
   a. SI ¨ Es requerido[76]" Revisión de la Seguridad Física
   b. SI ¨ Es requerido y aplica[77]" Revisión de Servidores UNIX
   c. SI ¨ Es requerido y aplica[78]" Revisión de Servidores y Estaciones Windows
   d. SI ¨ Es requerido y aplica[79]" Revisión de Servidores Sendmail
   e. SI ¨ Es requerido y aplica[80]" Revisión de Servidores Apache
   f. SI ¨ Es requerido y aplica[81]" #0.0.0.Revisión de la Infraestructura Inalámbricaloutline
   g. SI ¨ Es requerido y aplica[82]" Revisión del Sistema de Detección de Intrusos
   h. SI ¨ Es requerido y aplica[83]" Revisión de Dispositivos Firewalls
   i. SI ¨ Es requerido[84]" Revisión de las Políticas de Seguridad

[76] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. No depende de ningún otro tipo de condiciones.

[77] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. Aplica si existen servidores UNIX ó Linux.

[78] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. Aplica si existen servidores ó estaciones Windows.

[79] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. Aplica si existen servidores Sendmail.

[80] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. Aplica si existen servidores Apache cualquiera sea su versión. La versión es importante pues los servidores Apache v2 tienen características diferentes a los correspondientes a cualquiera de las subversiones 1.

[81] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. Aplica si existen servicios inalámbricos.

[82] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. Aplica si existen Detectores de Intrusos basados en host ó en red (Host DIS ó NDIS)

[83] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. Aplica si existen dispositivos firewalls gateways . No se refiere a firewalls personales que se auditan en la sección Revisión de Servidores y Estaciones Windows.

[84] Se refiere a que la función "Definición Inicial de los condiciones del proceso de auditoría" produzca la necesidad de realizar este tipo de revisiones. Aplica si existen Políticas de Seguridad "de facto", establecidas, no cumplidas, completas o incompletas.

Revisión de la Seguridad Física.

Objetivo de esta sección: Realizar revisión de las condiciones físicas que pudiesen influir en la continuidad operativa de las funciones de IT.

Salida : Inventario completo de las vulnerabilidades encontradas y recomendaciones de solución.

DESARROLLO:

1. PARA " Verificar la seguridad física del ambiente de cómputo y comunicaciones"

1.1 Verificar que los equipos se encuentren en ambientes adecuados en cuanto a: control temperatura y humedad, limpieza, aislamiento de cargas electrostáticas, protección contra descargas eléctricas, protección contra sismos.

1.2 SI "la prueba falla[85]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.

1.3 Verificar si existen medidas para Restringir y controlar el acceso a los dispositivos de cómputo central y de comunicaciones, cualquiera sea la plataforma de procesamiento.

1.4 SI "la prueba falla[86]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.

1.5 Verificar si existen equipos que permitan respuesta automática ante condiciones de riesgos como intrusiones físicas, incendios, temblores, aumentos buscos de la temperatura.

1.6 SI "la prueba falla[87]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.

1.7 Verificar que existan mecanismos para proteger físicamente[88] los respaldos de información.

1.8 SI "la prueba falla[89]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.

1.9 Verificar si existen planes de contingencia para el mantenimiento operativo ante la materialización de situaciones de riesgo físico como las mencionadas en los acápites anteriores.

1.10 SI "la prueba falla[90]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.

1.11 Verificar que existan mecanismos adicionales para la continuidad del suministro eléctrico a los centros de carga principales y que estos sistemas funcionen adecuadamente.

1.12 SI "la prueba falla[91]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.

---

85 Falla de la prueba significa que alguno de los parámetros que se mencionan en este acápite no se cumple.

86 Falla de la prueba significa que alguno de los parámetros que se mencionan en este acápite no se cumple.

87 Falla de la prueba significa que alguno de los parámetros que se mencionan en este acápite no se cumple.

88 Proteger los respaldos significa evitar su destrucción parcial o total de manera accidental, por acción de elementos ambientales o por acciones deliberadamente malintencionadas.

89 Falla de la prueba significa que alguno de los parámetros que se mencionan en este acápite no se cumple.

90 Falla de la prueba significa que no existen planes de continuidad operativa o estos no son correctos o completos.

91 Falla de la prueba significa que alguno de los parámetros que se mencionan en este acápite no se cumple.

1.13 Verificar que existen planes de evacuación ante emergencias del personal y resguardo de los equipos principales ante la ocurrencia de imprevistos que lo ameriten.
1.14 SI "la prueba falla[92]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.
1.15 Verificar que el personal conoce y ha sido entrenado para utilizar los planes de contingencia mencionados en el no. 5.
1.16 SI "la prueba falla[93]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.
1.17 Verificar que los sistemas de suministro eléctrico se encuentren adecuadamente dimensionados y protegidos.
1.18 SI "la prueba falla[94]" ENTONCES Recomendar corregir las condiciones de riesgos encontradas.

[92] Falla de la prueba significa que alguno de los parámetros que se mencionan en este acápite no se cumple.
[93] Falla de la prueba significa que alguno de los parámetros que se mencionan en este acápite no se cumple.
[94] Falla de la prueba significa que alguno de los parámetros que se mencionan en este acápite no se cumple.

Revisión de Servidores Unix

Objetivo de esta sección: Realizar revisión de la configuración de servidores Unix y Linux que afecten condiciones de riesgo de seguridad.
Durante esta revisión se buscan condiciones de riesgos que pudieron no ser develadas durante las pruebas de penetración.

Salida : Inventario completo de las vulnerabilidades encontradas y recomendaciones de solución.

DESARROLLO:

I. PARA " Realizar Revisión de Sistemas Basados en Unix"
   A. Por cada servidor o estación a auditar {
      i. Verificar Seguridad del Sistema de Archivos
      ii. Verificar los procesos activos, su forma de inicio y la seguridad básica de los mismos
      iii. Verificar la Seguridad de Contraseñas
      iv. Verificar la seguridad del sistema de manejo de usuarios
      v. Verificar la efectividad y seguridad del sistema de respaldos
      vi. Verificar la efectividad y seguridad del sistema de detección de intrusos
      vii. Verificar la efectividad y seguridad del sistema de bitácoras
      viii. Verificar la efectividad y seguridad del sistema de control de acceso
      ix. SI "se utiliza NFS" ENTONCES Verificar la efectividad y seguridad del sistema de directorios NFS }

1 PARA "Verificar Seguridad del Sistema de Archivos"

1.1 Verificar que las opciones de montaje del sistema de Archivos impida que cualquier usuario pueda montar o desmontar otros sistemas de archivos. SI "la prueba falla[95]" ENTONCES Recomendar urgentemente corregir la configuración permisos de montaje.

1.2 Buscar programas con SUID o SGID activados y comparar con lista de programas permitidos (VER ANEXO UNIX-1) .

[95] Falla de la prueba significa que cualquier usuario sin permisos especiales pueda montar/desmontar otros sistemas de archivos.

1.3 SI "la prueba falla[96]" ENTONCES Recomendar revisar la razón del aumento de permisología de los programas detectados.

1.4 Verificar permisología de programas de configuración en /etc, /usr/local.

1.5 SI "la prueba falla[97]" ENTONCES Recomendar corregir los errores de asignación de permisología

1.6 Verificar permisología de los directorios home de cada usuario. SI "la prueba falla[98]" ENTONCES Recomendar corregir los errores de asignación de permisología

1.7 SI "el de archivos admite el uso de ACL " ENTONCES Verificar si existen listas de acceso para programas de administración principales y son correctas. SI "la prueba falla[99]" ENTONCES Recomendar corregir los errores de asignación de permisología

1.8 Verificar si se utiliza el comando umask y si la permisología asignada es correcta. SI "la prueba falla[100]" ENTONCES Recomendar corregir los errores de asignación de permisología

1.9 Verificar que no existan shell scripts con permisología SUID o SGID. SI "la prueba falla[101]" ENTONCES Recomendar corregir los errores de asignación de permisología de los scripts detectados.

2 PARA "Verificar los procesos activos, su forma de inicio y la seguridad básica de los mismos"

2.1 Verificar que procesos se están ejecutando sólo los procesos que se ajustan a las funciones del servidor. SI "la prueba falla[102]" ENTONCES Recomendar mantener ejecutándose sólo los servicios necesarios.

2.2 Verificar que el proceso de inicio de los procesos sea correcto. SI "la prueba falla[103]" ENTONCES Recomendar revisar los scripts de arrancada se servicios.

2.3 Verificar que los scripts de arrancada tenga la permisología correcta y no puedan ser invocados por usuarios normales. SI "la prueba falla[104]" ENTONCES Recomendar verificar la permisilogía de los scripts de arrancada.

2.4 Verificar que los usuarios no pueden ejecutar servicios sin control del administrador del sistema. SI "la prueba falla[105]" ENTONCES Recomendar ajustar los niveles de control para impedir esta situación.

---

96 Falla de la prueba significa que se encuentren programas con permisos SUID/SGID que no justifiquen esta permisólogía. Es importante que la guía que se muestra al final de esta sección se utilice sólo como referencia.

97 Falla de la prueba significa que se encuentren en los subdirectorios donde existan archivos de configuración permisos erróneos que permitan

98 Falla de la prueba significa que se encuentren en los subdirectorios home cuya permisólogía sea incorrecta.

99 Falla de la prueba significa que se encuentren listas de acceso incorrectamente configuradas.

100 Falla de la prueba significa que se umask asigne por omisión permisos en exceso.

101 Falla de la prueba significa que se encuentren shells scripts con permisos SUID.

102 Falla de la prueba significa que se encuentren servicios activos que no son necesarios.

103 Falla de la prueba significa que se encuentren errores o irregularidades en los scripts de arrancada de los servicios.

104 Falla de la prueba significa que se encuentren errores en la permisólogía de los scripts de arrancada..

105 Falla de la prueba significa que cualquier usuario puede montar un servicio sin control del administrador.

2.5 POR CADA Servicio_Activo[106]

2.5.1 Verificar el mecanismo de invocación

2.5.1.1 SI "Mecanismo_Invocación es Inetd" ENTONCES verificar que se utilicen las opciones adecuadas de seguridad. SI "la prueba falla[107]" ENTONCES Recomendar ajustar los parámetros de ejecución del demonio.

2.5.2 Verificar que Versión actual se la Versión mas actualizada disponible de acuerdo a las políticas de uso del sitio auditado. SI "la prueba falla[108]" ENTONCES Recomendar actualizar la versión del servicio.

2.5.3 Verificar que exista control de acceso al servicio (por medio de ACL, Wrappers u otro mecanismo). SI "la prueba falla[109]" ENTONCES Recomendar actualizar los niveles de control de acceso.

2.5.4 Verificar que no tenga shell válido SI "la prueba falla[110]" ENTONCES Recomendar cambiar el shell a no válido.

2.5.5 Verificar que no tenga home válido. SI "la prueba falla[111]" ENTONCES Recomendar borrar el directorio $HOME no existente.

3 PARA " Verificar la Seguridad de Contraseñas"

3.1 Verificar si existen políticas de conformación de contraseñas.

3.2 Verificar si existen políticas de historial de contraseñas

3.3 Verificar si existen políticas de duración (máxima y mínima) de contraseñas

3.4 Verificar si existe shadow password

3.5 Verificar si todos los usuarios poseen contraseñas seguras[112]

3.6 Verificar que todos quienes usan el servidor tienen su propia cuenta

3.7 Verificar si existen programas de control de calidad de contraseñas

3.8 Verificar si existen mecanismos adicionales de control de acceso[113]

---

[106] Se refiere a los servicios que se estén ejecutando en el momento de realizar la auditoría

[107] Falla de la prueba significa los parámetros de seguridad no se utilicen para los demonios manejados por inetd. Válido para xinetd.

[108] Falla de la prueba significa que no se utiliza la versión más actualizada sin criterios válidos. Esta acción sólo debe recomendarse si la versión que se ejecuta posee vulnerabilidades.

[109] Falla de la prueba significa que se encuentren servicios activos que no son necesarios.

[110] Falla de la prueba significa que el usuario con que corre el demonio tiene en /etc/passwd un shell que permite a un usuario tomar su identidad y ejecutar comandos.

[111] Falla de la prueba significa que el usuario con que corre el demonio tiene en /etc/passwd un subdirectorio $HOME existente. > $HOME: /dev/null /$SHELL: sbin/nologin

[112] Utilizar un programa para rompimiento de claves

[113] OTP, smartcard, certificación digital

3.9 SI "la prueba falla[114]" ENTONCES Recomendar revisar la política de contraseñas.

4 PARA "Verificar la seguridad del sistema de manejo de usuarios"

4.1 Verificar que varios usuarios no comparten el mismo UID

4.2 Verificar que la cuenta root no se utiliza para actividades regulares

4.3 Verificar si existen restricciones al uso del comando su

4.4 Verificar quienes pertenecen al grupo 0

4.5 Verificar que los usuarios no tienen archivos ./rhost[115]

4.6 Verificar que el .[116] no se encuentra en la variable $PATH

4.7 Verificar si existen restricciones al uso del comando sudo

4.8 Rastrear los archivos de bitácoras en búsqueda de intentos de escalada de privilegios

4.9 Verificar que no existan cuentas dormidas habilitadas.

4.10 SI "la prueba falla[117]" ENTONCES Recomendar revisar la política de seguridad de usuarios.

4.11 SI "se utiliza LDAP" ENTONCES verificar se utilice Kerberos ó MD5 Hash como mecanismos de autenticación.

4.11.1 SI "la prueba falla[118]" ENTONCES Recomendar revisar la política de autentificación de usuarios.

4.12 SI "se utiliza LDAP" ENTONCES Verificar la información entre clientes y servidores viaje cifrada.

4.12.1 SI "la prueba falla[119]" ENTONCES Recomendar utilizar mecanismos de cifrado de la información que incluyan el paso de credenciales entre clientes y servidores.

5 PARA "Verificar la efectividad y seguridad del sistema de respaldos"

5.1 Verificar regularidad de los respaldos

5.2 Verificar política de respaldos

5.3 Verificar si se respaldan los archivos importantes del sistema

[114] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados en los acápites del 3.1 al 3.8

[115] Especialmente root

[116] Se refiere al directorio actual.

[117] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.

[118] Falla de la prueba significa que se se utilizan PLAIN ó LOGIN como vías de autentificación.

[119] Falla de la prueba significa no se cifra el canal de datos ó no se cifran las credenciales entre clientes y servidores.

5.4 Verificar si la política de respaldo incluye la verificación de los mismos

5.5 Verificar política de almacenamiento y cuidado de respaldos

5.6 Verificar si existen varias formas de respaldo de la información completa

5.7 SI "la prueba falla[120]" ENTONCES Recomendar revisar la politica de respaldos.

6 PARA "Verificar la efectividad y seguridad del sistema de detección de intrusos"

6.1 Verificar si existen programas "IDS Target", si se ejecutan con regularidad y si sus resultados son atendidos correctamente. SI "la prueba falla[121]" ENTONCES Recomendar revisar la detección de intrusos.

6.2 SI existen programas "IDS Target" ENTONCES Verificar que se protejan los archivos adecuados. SI "la prueba falla[122]" ENTONCES Recomendar revisar la configuración de los sistemas de detección de intrusos.

6.3 Verificar si existen programas IDS Host, si se ejecutan con regularidad y si sus resultados son atendidos correctamente. SI "la prueba falla[123]" ENTONCES Recomendar revisar la detección de intrusos a nivel de hosts.

6.4 SI "existen programas "IDS host " ENTONCES Verificar que se revisen los archivos adecuados. SI "la prueba falla[124]" ENTONCES Recomendar revisar la configuración de los sistemas de detección de intrusos.]

7 PARA "Verificar la efectividad y seguridad del sistema de bitácoras"

7.1 Verificar que exista el adecuado nivel de bitácoras

7.2 Comprobar si las bitácoras están debidamente protegidas

7.3 Comprobar si todos los servicios tienen servicios de bitácoras

7.4 Verificar si las bitácoras se rotan

7.5 Verificar si las bitácoras se respaldan en otros servidores (syslog)

7.6 Verificar si se lleva registro sobre los acceso a las bitácoras

7.7 SI "la prueba falla[125]" ENTONCES Recomendar revisar la política de bitácoras.

8 PARA "Verificar la efectividad y seguridad del sistema de control de acceso"

[120] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[121] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[122] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[123] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[124] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[125] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.

8.1 Verificar si existen filtrado paquetes[126] y de nivel de aplicaciones[127]. SI "la prueba falla[128]" ENTONCES

8.1.1 Recomendar revisar políticas de control de acceso y Revisar que los mecanismos establecidos filtren adecuadamente el acceso a las aplicaciones.

8.1.1.1 SI "la prueba falla[129]" ENTONCES Recomendar revisar la configuración de los sistemas de control de acceso.

8.2 Revisar que los mecanismos establecidos registren adecuadamente los intentos de acceso tanto satisfactorios como fallidos. SI "la prueba falla[130]" ENTONCES Recomendar revisar la configuración de los sistemas de control de acceso.

9 PARA "Verificar la efectividad y seguridad del sistema de directorios NFS"

9.1 Verificar que todas las exportaciones del sistema de archivos se realizan hacia destinos y usuarios estrictamente definidos. SI "la prueba falla[131]" ENTONCES Recomendar ajustar el sistema de exportación para evitar esta situación.

9.2 Verificar que el sistema obliga a los clientes a usar puertos privilegiados. SI "la prueba falla[132]" ENTONCES Recomendar revisar la configuración del sistema NFS.

9.3 Verificar que el sistema utiliza las opciones cross-check PTR y ADDR hostname lookups[133]. SI "la prueba falla[134]" ENTONCES Recomendar revisar la configuración del sistema NFS

10 PARA "Verificar la efectividad y seguridad del sistema NIS"

10.1 Verificar si sólo se exportan mapas a estaciones de confianza. SI "la prueba falla[135]" ENTONCES Recomendar revisar la configuración del sistema NIS.

10.2 Verificar si se utiliza "+:" en lugar de "+::0:0:::" como marca en el archivo de passwords. SI "la prueba falla[136]" ENTONCES Recomendar reajustar el parámetro en el archivo password.

10.3 Verificar que los mapas NIS sean sólo modificables por el root. SI "la prueba falla[137]" ENTONCES Recomendar ajustar la permisología de los archivos.

---

[126] firewalls locales
[127] wrappers, inetd.
[128] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[129] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[130] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[131] Falla de la prueba significa que se encuentran en /etc/fstab partes del sistema de archivos exportados a everyone.
[132] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[133] Impiden DNS spoofing
[134] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[135] Falla de la prueba significa que se encuentran deficiencias en alguno de los parámetros revisados.
[136] Falla de la prueba significa que se la marca incorrecta en el archivo mencionado
[137] Falla de la prueba significa que los mapas maestros puedan ser modificados sin permisología root.

Revisión de Servidores y Estaciones Basados Windows

Objetivo de esta sección: Realizar revisión de la configuración de las estaciones y servidores con sistemas operativos de la familia Windows.
Durante esta revisión se buscan condiciones de riesgos que pudieron no ser develadas durante las pruebas de penetración.

Salida : Inventario completo de las vulnerabilidades encontradas y recomendaciones de solución.

DESARROLLO:

I. PARA " Revisar Servidores y Estaciones basadas en Windows"
   A. Por cada estación ó servidor a auditar {
      i. Verificar la seguridad del sistema control de usuarios y contraseñas
      ii. SI "Es un servidor y se utiliza AD" ENTONCES Verificar los atributos de Active Directory (AD)
      iii. Verificar la existencia de permisología mínima
      iv. Verificar la seguridad de la configuración básica los servicios y las actualizaciones
      v. Verificar la protección del stack TCPIP
      vi. Verificar la efectividad y seguridad del sistema de auditoría interna
      vii. SI " es un servidor y el servidor es un servidor de dominios" ENTONCES Verificar la seguridad de la configuración básica de controladores de dominios
      viii. SI " es un servidor y el servidor es un servidor DNS" ENTONCES Verificar la efectividad y seguridad de los servidores DNS
      ix. SI " es un servidor y el servidor es Terminal Server" ENTONCES Verificar la seguridad de la configuración básica del servicio Terminal Server (TS)
      x. SI " es un servidor y el servidor es DHCP Server" ENTONCES Verificar seguridad de la configuración básica de los servidores DHCP
      xi. SI " es un servidor y el servidor es WINSServer" ENTONCES Verificar seguridad de servidores WINS }

1 PARA "Verificar la seguridad del sistema control de usuarios y contraseñas"

1.1 Verificar que no se utilizan cuantas administrativas para trabajo cotidiano.

1.2 Verificar la existencia de usuarios sin contraseñas.SI "la prueba falla[138]" ENTONCES Recomendar ajustar urgentemente las políticas de contraseñas de usuarios para evitar la situación detectada.

1.3 Verificar la existencia de usuarios que nunca han usado su cuenta. SI "la prueba falla[139]" ENTONCES Recomendar ajustar urgentemente las políticas de contraseñas de usuarios para evitar la situación detectada.

1.4 SI "la prueba falla[140]" ENTONCES Recomendar corregir esta situación.

1.5 SI "Versión del SO >=windows nt 4 SP 2 Y el sistema es un servidor crítico" ENTONCES Verificar uso syskey en niveles superiores a 1. SI "la prueba falla[141]" ENTONCES Recomendar utilizar syskey nivel 2 ó 3.

1.6 SI "Version del SO < windows nt 4 SP 2" ENTONCES Recomendar actualización urgente que permita el uso de syskey[142].

1.7 Verificar que no se asignan permisos directamente a las cuentas. SI "la prueba falla[143]" ENTONCES Recomendar utilizar grupos en lugar de cuentas individuales.

1.8 Verificar Privilegios de usuarios buscando privilegios mínimos. SI "la prueba falla[144]" ENTONCES Recomendar ajustar urgentemente los privilegios de usuarios para evitar la situación detectada

1.9 Verificar Derechos de Inicio de Sesión. SI "la prueba falla[145]" ENTONCES Recomendar ajustar urgentemente los privilegios de usuarios para evitar la situación detectada.

1.10 Verificar (rompiendo) longitud y calidad de las contraseñas. SI "la prueba falla[146]" ENTONCES Recomendar ajustar urgentemente la política de contraseñas (VER ANEXO WIN-1)de usuarios para evitar la situación detectada.

1.11 Verificar la existencia de errores en la política de contraseñas. SI "la prueba falla[147]" ENTONCES

[138] Falla de la prueba significa se han encontrado usuarios sin claves.

[139] Falla de la prueba significa se han encontrado usuarios que nunca han accesado su cuenta.

[140] Falla de la prueba significa se encuentra al menos un equipo en el cual los usuarios utilizan la cuentas con permisos administrativos para trabajo regular.

[141] Falla de la prueba significa que sólo se utiliza syskey 1 (valor por omisión para el ambiente)

[142] Syskey se utiliza desde el services pack 2 de Windows NT.

[143] Falla de la prueba significa que no se utilizan grupos para la asignación de privilegios.

[144] Falla de la prueba significa se han encontrado usuarios con privilegios no adecuados a la función que realizan.

[145] Falla de la prueba significa que se han detectado usuarios que poseen permisos de inicio de sesión que no deberían. Ej. usuarios del sistema, usuarios que no pertenecen a la organización, usuarios de otros dominios, unidades organizativas, etc...

[146] Falla de la prueba significa se han encontrado usuarios con contraseñas débiles. Para realizar esta acción es conveniente utilizar una herramienta especializada de rompimiento de contraseñas. Ej LC4 y pwdump (ver sección de Pruebas de Penetración).

[147] Falla de la prueba significa que se encuentre errores como: No se mantiene historial de las contraseñas, las contraseñas no tiene definidos tiempos de vida (máximo y mínimo), tamaño mínimo, conformación de la contraseña

Recomendar ajustar urgentemente las políticas de contraseñas de usuarios para evitar la situación detectada.

1.12 Verificar que no se utilicen algoritmos de hash de LM[148]. SI "la prueba falla[149]" ENTONCES Recomendar ajustar urgentemente la política de autentificación y utilizar NTLMv2.

1.13 SI "la versión de SO es 200X[150] ó XP" ENTONCES Verificar si se utiliza Kerberos.

1.13.1 SI "la prueba falla" ENTONCES Verificar si es posible utilizar Kerberos [151].

1.13.2 SI "la prueba falla[152]" ENTONCES Recomendar ajustar urgentemente la política de autentificación y utilizar Kerberos.

1.13.3 Verificar nivel de cache de contraseñas. SI "la red es de alta seguridad y el nivel de cache es diferente de 0. ENTONCES Recomendar llevar el nivel de cache a 0.

2 PARA "Verificar los atributos de Active Directory (AD)"

2.1 Verificar que no se utilicen permisos a grupos locales de dominio. SI "la prueba falla[153]" ENTONCES Recomendar asignar los permisos a todo el bosque mediante grupos universales.

2.2 Verificar quienes tiene acceso como Administradores del bosque y validar que no se tienen permisos excesivos a este nivel. SI "la prueba falla[154]" ENTONCES Recomendar ajustar urgentemente la política de asignación de permisos.

2.3 Verificar que existe protección física para los controladores de dominio raíz del bosque. SI "la prueba falla[155]" ENTONCES Recomendar corregir urgentemente la política de protección física de los controladores de dominio raíz.

2.4 SI se requiere aislamiento discreto de funciones y existe un sólo bosque ENTONCES Recomendar utilizar varios bosques.

2.5 Verificar si los administradores de AD utilizan estaciones de trabajo particulares para las funciones de administración. SI "la prueba falla[156]" ENTONCES Recomendar corregir la práctica detectada.

---

148 Puede ser que por necesidad de mantener compatibilidad con aplicaciones antiguas sean necesario mantener LanManager, sin embargo esta situación debe ser especialmente evualuada.

149 Falla de la prueba significa que no existen justificaciones para mantener contraseñas LM

150 Windows 2000 ó 2003

151 Kerberos sólo puede ser utilizado si se tiene un ambiente completo en XP ó 200X

152 Falla de la prueba significa que no existen justificaciones para no usar Kerberos

153 Falla de la prueba significa los permisos se otorgan a grupos locales del dominio que sólo son válidos en ese contexto.

154 Falla de la prueba significa que los administradores de bosques tiene tambien permisos en otras unidades de la estructura de AD.

155 Falla de la prueba significa que puede ser comprometida la seguridad física de los controladores de dominio raíz, lo cual podría implicar la pérdida de todos los dominios hijos del servidor que pueda ser comprometido.

156 Falla de la prueba significa que los administradores no utilizan estaciones particulares y seguras para funciones de administración , haciéndose vulnerables a ataques en a las estaciones clientes que utilizan

2.6 Verificar si se delegan autoridades sobre las unidades organizativas (u objetos) en lugar de designar permisos específicos para cada una. SI "la prueba falla[157]" ENTONCES Recomendar corregir la práctica detectada.

2.7 Verificar si se utiliza DNS integrado a Active Directory. SI "la prueba falla[158]" ENTONCES Recomendar corregir la práctica detectada.

2.8 Verificar se utilice Kerberos ó MD5 Hash como mecanismos de autenticación. SI "la prueba falla[159]" ENTONCES Recomendar revisar la política de autentificación de usuarios.

2.9 Verificar la información entre clientes y servidores viaje cifrada. SI "la prueba falla[160]" ENTONCES Recomendar utilizar mecanismos de cifrado de la información que incluyan el paso de credenciales entre clientes y servidores.

3 PARA "Verificar la existencia de permisología mínima".

3.1 Verificar los permisos mínimos según la función. SI "la prueba falla[161]" ENTONCES Recomendar corregir la práctica detectada.

3.2 Verificar si se utilizan mecanismos de cifrado para la data sensitiva. SI "la prueba falla[162]" ENTONCES Recomendar corregir la práctica detectada.

3.3 Verificar los permisos del registro del sistema. SI "la prueba falla[163]" ENTONCES Recomendar corregir los errores de permisología encontrados.

4 PARA "Verificar la seguridad de la configuración básica de los servicios y las actualizaciones"

4.1 Verificar que no existan servicios superfluos o no convencionales ejecutándose. SI "la prueba falla[164]" ENTONCES Recomendar corregir los errores de permisología encontrados.

4.2 Verificar si se han instalado los parches más recientes. SI "la prueba falla[165]" ENTONCES Recomendar corregir los errores de permisología encontrados

5 PARA "Verificar la protección del stack TCP/IP"

5.1 SI el "SO es "Windows 2000" ó "Windows XP" ó "Windows 2003"" ENTONCES

5.1.1 En el registro del sistema verificar

5.1.1.1 EnableICMPRedict=0

[157] Falla de la prueba significa que el manejo de permisos se realiza de manera individual y no utilizando las funciones de delegación de privilegios.

[158] Falla de la prueba significa el DNS se utiliza de manera separada del AD, lo cual reduce la seguridad del servicio.

[159] Falla de la prueba significa que se se utilizan PLAIN ó LOGIN como vías de autentifiación.

[160] Falla de la prueba significa no se cifra el canal de datos ó no se cifran las credenciales entre clientes y servidores.

[161] Falla de la prueba significa que se han encontrado plantillas de permisos mas permisivas que las planteadas en el anexo W-1

[162] Falla de la prueba significa la información sensible que pueda estar contenida en algún servidor no es cifrada.

[163] Falla de la prueba significa que los permisos del registro de windows no cumplen con los requerimientos mínimos.

[164] Falla de la prueba significa existen servicios que no deberían estar ejecutándose o cuya función no puede ser establecida

[165] Falla de la prueba significa que existen equipos no actualizados.

5.1.1.2 SynAttackProtect =2

5.1.1.3 TCPMaxConnectResponseRetransmition=2

5.1.1.4 TCPMaxHalfOpen=50

5.1.1.5 TCPMaxHalfOpenRetired=400

5.1.1.6 TCPMaxPortsExhauted=5

5.1.1.7 TCPMaxDataRetransmitions=3

5.1.1.8 EnableDeagGWDetect=0

5.1.1.9 EnablePMTUDiscovery=0

5.1.1.10 DisableIPSourceRouting=2

5.1.1.11 NoNameReleaseonDemand=1

5.1.1.12 PerfomRouterdiscovery=0

5.1.2 SI "5.1.1 falla[166]" ENTONCES Recomendar corregir la configuración errónea.

5.2 SI "SO es "Windows 2000" ó "Windows XP" ó "Windows 2003" Y "están habilitados los servicios FTP ó HTTP" ENTONCES

5.2.1 En el registro del sistema verificar:

5.2.1.1 EnableDynamicBacklog=1

5.2.1.2 dynamicBlacklogGrowthDelta=10

5.2.1.3 MinimumdynamicBlacklog=20

5.2.1.4 MaximunDynamicBlacklog=20.000

5.2.2 SI "5.2.1 falla[167]" ENTONCES Recomendar corregir la configuración errónea.

6 PARA "Verificar la efectividad y seguridad del sistema de auditoría interna"

6.1 SI SO > Windows NT ENTONCES Verifica si las políticas de auditoría están habilitadas.

6.2 SI "La prueba falla[168]" ENTONCES Recomendar corregir la configuración errónea

6.3 DE LO CONTRARIO ENTONCES

6.3.1 Verificar SI

6.3.1.1 Se auditan[169] sucesos de inicio de sesión o

[166] Falla de la Prueba significa que alguno de los parámetros evaluados tiene un valor incorrecto y que no puede ser justificado por las necesidades operativas de los equipos.

[167] Falla de la Prueba significa que alguno de los parámetros evaluados tiene un valor incorrecto y que no puede ser justificado por las necesidades operativas de los equipos.

[168] Falla de la Prueba significa no se encuentran habilitadas los procesos de auditoría del Sistema Operativo.

[169] Aquí se debe auditar no sólo los eventos exitosos sino también los intentos infructuosos de realizar la acción. Válido para todas las comprobaciones de esta sección.

6.3.1.2 Se audita la administración de cuentas o

6.3.1.3 Se audita el acceso a los servicios de directorios o

6.3.1.4 Se auditan acceso a objetos de SO

6.3.1.5 Se audita el cambio de directivas

6.3.1.6 Se audita el uso de privilegios

6.3.1.7 Se audita el seguimiento de procesos

6.3.1.8 Se auditan sucesos del sistema

6.3.2 SI "la prueba falla" [170] ENTONCES Recomendar corregir las configuraciones incorrectas.

7 PARA "Verificar la seguridad de la configuración básica de controladores de dominios"

7.1 Verificar que no se utilicen aplicaciones con contraseñas cifradas con algoritmos de doble vía.

7.2 SI "La prueba falla[171]" ENTONCES Recomendar corregir la configuración errónea.

7.3 SI "existen más de un controlador de dominios" ENTONCES verificar que todos pertenezcan a una unidad organizativa común.

7.3.1 SI "La prueba falla[172]" ENTONCES Recomendar corregir la configuración errónea

7.4 Verificar si existen una plantilla de seguridad de línea base y si esta se aplica a la unidad organizativa a la que pertenecen los servidores de dominio. SI "La prueba falla[173]" ENTONCES Recomendar corregir la configuración errónea

7.5 Verificar si las plantillas de seguridad son almacenadas de forma segura. SI "La prueba falla[174]" ENTONCES Recomendar corregir la configuración errónea

8 PARA "Verificar la efectividad y seguridad de los servidores DNS

8.1 Verificar si existen zonas integradas a AD. (ver punto 2.7)

8.2 Verificar si los servidores internos y externos son independientes.

8.3 SI "La prueba falla[175]" ENTONCES Recomendar corregir la configuración errónea

[170] Falla de la prueba significa que alguno de los elementos de autoría no se registran o su registro es incorrecto.

[171] Falla de la Prueba significa las contraseñas pueden ser descifradas utilizando DES en lugar de tener que ser "adivinadas" utilizando un proceso de fuerza bruta.

[172] Falla de la Prueba significa que se han creado varios bosques sin un punto común de unión, lo cual dificulta la administración y la difusión de políticas.

[173] Falla de la Prueba significa que se no se han aplicado las medidas mínimas de seguridad recomendadas por el fabricante.

[174] Falla de la Prueba significa que las plantillas de seguridad no son protegidas de cambios y destrucción accidental o mal intencionada. Una plantilla modificada podría relajar los controles de toda la red, entorpecer su funcionamiento o incluso dejarla in-operativa.

[175] Falla de la Prueba significa no existe división entre los servidores que anuncian la red hacia el mundo y aquellos que realizan la función internamente. Esta configuración facilita la enumeración de la red desde el exterior.

8.4 Verificar si existen restricciones a las transferencias de zonas.

8.5 SI "La prueba falla[176]" ENTONCES Recomendar corregir la configuración errónea

8.6 Verificar quienes y porque pertenecen al grupo DNSAdmin. SI "La prueba falla[177]" ENTONCES Recomendar corregir la configuración errónea

9 PARA " Verificar la seguridad de la configuración básica del servicio Terminal Server (TS)"

9.1 Verificar si la plantilla de seguridad Notssid.inf está aplicada servidores con permisos compatibles con Terminal Server 4.0. SI "La prueba falla[178]" ENTONCES Recomendar corregir la configuración errónea.

9.2 Verificar que se ha restringido las aplicaciones disponibles para usuarios de TS. SI "La prueba falla[179]" ENTONCES Recomendar corregir la configuración errónea

9.3 Verificar que no está habilitado el control remoto en los servidores de TS. SI "La prueba falla[180]" ENTONCES Recomendar corregir la configuración errónea

9.4 Verificar que está habilitado High Encryption Pack. SI "La prueba falla[181]" ENTONCES Recomendar aumentar el nivel de cifrado de las operaciones de TS.

10 PARA "Verificar seguridad de la configuración básica de los servidores DHCP"

10.1 Verificar que no exista la cuenta del servidor en el grupo DNSUpdateProxy. SI "La prueba falla[182]" ENTONCES Recomendar corregir la configuración errónea

10.2 Verificar que no se utilicen direcciones asignadas por DHCP para servidores. SI "La prueba falla[183]" ENTONCES Recomendar corregir la configuración errónea

10.3 Verificar quienes y por qué pertenecen al grupo Administradores DHCP. SI "La prueba falla[184]" ENTONCES Recomendar corregir la configuración errónea

[176] Falla de la Prueba significa no existe restricciones a las transferencias de zonas de DNS lo que facilita la enumeración de la red desde el exterior.

[177] Falla de la Prueba significa existen usuarios dentro del grupo DNSAdmin que pudiesen cambiar accidental o mal intencionadamente la configuración de DNS sin control del administrador del sistema.

[178] Falla de la Prueba significa el servicio Terminal Server es vulnerable a varios ataques por aplicación errónea de la permisología de usuarios.

[179] Falla de la Prueba significa no existe restricciones a lo que los usuarios de acceso remoto pueden hacer. Debido a la debilidad intrínseca de este servicio se recomienda restringir explícitamente lo que se permite hacer a los usuarios del mismo.

[180] Falla de la Prueba significa que están habilitadas funciones o programas de control remoto. Todas estas aplicaciones son no recomendadas a no ser que se utilicen sobre canales seguros de comunicación tales como VPN. Aún en el último caso debe tenerse cuidado al usarse pues podría dejar inoperativo el servidor.

[181] Falla de la Prueba significa que no se implementa cifrado o este es muy débil para considerarse seguro.

[182] Falla de la Prueba significa que el servidor pertenece al grupo señalado lo cual impide que el servidor tome posesión de los registros que incorpore al DNS. Esta situación es sólo válida si existen mas de un servidor DHCP en el dominio.

[183] Falla de la Prueba significa los servidores podrán cambiar sus direcciones IP al cambiar la asignación que se les hace vía DHCP.

[184] Falla de la Prueba significa existen usuarios dentro del grupo Administradores DHCP que pudiesen cambiar accidental o mal intencionadamente la configuración de DNS sin control del administrador del sistema.

10.4 Verificar que está habilitada la auditoría de DHCP. SI "La prueba falla[185]" ENTONCES Recomendar corregir la configuración errónea

11 PARA "Verificar seguridad de servidores WINS"

11.1 Verificar la necesidad de mantener servidores WINS dentro del dominio[186]. SI "La prueba falla[187]" ENTONCES Recomendar corregir la configuración errónea

11.2 SI "es necesario mantener WINS" ENTONCES Recomendar que exista el número mínimo de servidores WINS dentro del domino.

11.3 Verificar las replicaciones entre servidores WINS. SI "La prueba falla[188]" ENTONCES Recomendar corregir la configuración errónea

[185] Falla de la Prueba significa que el servicio de auditoría no registra los eventos del servidor DHCP.

[186] WINS es un protocolo obsoleto y en desuso. AD su integración con DNS lo hacen innecesario.

[187] Falla de la Prueba significa no existen justificaciones válidas para mantener WINS funcionando. WINS es un servicio arcaico y ha sido suplantado por AD.

[188] Falla de la Prueba significa que se encuentran servidores WINS que no registran sus operaciones en el resto de los servidores WINS.

Revisión de Servidores Sendmail

Objetivo de esta sección: Realizar revisión de la configuración de servidores que ejecuten sendmail como demonio manejador de correo electrónico.
Durante esta revisión se buscan condiciones de riesgos que pudieron no ser develadas durante las pruebas de penetración.

Salida : Inventario completo de las vulnerabilidades encontradas y recomendaciones de solución.

I. PARA "Revisar Servidores Sendmail" {

A. Verificar que la versión utilizada no contenga errores insuperables
B. Verificar las condiciones generales de funcionamiento del servicio
C. Verificar la efectividad y seguridad de las técnicas Anti-Relay
D. Verificar existencia de servicios de autentificación
E. Verificar la efectividad y seguridad de las técnicas de prevención de ataques del tipo DoS
F. Verificar la seguridad de otras opciones }

1 PARA "Verificar que la versión utilizada no contenga errores insuperables"
1.1 SI " Versión del sendmail <= 8.9.3" ENTONCES Abortar Auditoría[189] y Recomendar actualizar de manera inmediata el sendmail.
1.2 SI Versión_Demonio < versión_mas_actualizada_estable ENTONCES Recomendar Actualización de la versión.

2 PARA "Verificar las condiciones generales de funcionamiento del servicio"

2.1 Verificar con que usuario corre el demonio. [190] y Verificar que nadie mas pertenece al grupo. SI "la prueba falla[191]" ENTONCES Recomendar urgentemente corregir la situación.

2.2 Verificar que el usuario de sendmail no tiene shell válido. SI "la prueba falla[192]" ENTONCES Recomendar urgentemente corregir la situación.

2.3 Verificar permisología[193] básica de los archivos de configuración y colas de sendmail.

[189] Cualquier versión anterior a 8.9.3 debe ser completamente sustituida, no vale la pena auditar
[190] Debe ser smmsp:smmsp (osimilar)
[191] Falla de la prueba significa que alguien más pertenece al grupo del usuario con que corre sendmail.
[192] Falla de la prueba significa que el usuario con que corre el demonio tiene en /etc/passwd un shell que permite a un usuario tomar su identidad y ejecutar comandos.
[193] Esta revisión se ha realizado en la sección Revisión de Servidores UNIX.

2.4 Chequear Alias buscando entradas sospechosas[194]. SI "la prueba falla[195]" ENTONCES Recomendar urgentemente corregir la situación.

2.5 Verificar los programas que pueden ser utilizados por el MTA en el smrsh. SI "la prueba falla[196]" ENTONCES Recomendar urgentemente corregir la situación.

2.6 Verificar permisos de archivos forward[197]. SI "la prueba falla[198]" ENTONCES Recomendar urgentemente corregir la situación.

2.7 Verificar que cualquier usuario no pueda ver el estado de las colas de correos.[199] SI "la prueba falla[200]" ENTONCES Recomendar corregir esta situación.

3 PARA "Verificar la efectividad y seguridad de las técnicas Anti-Relay[201]"

3.1 Verificar que no exista FEATURE ('relay_entire_domain'). SI "la prueba falla[202]" ENTONCES Recomendar corregir esta situación.

3.2 Verificar que no exista FEATURE(`promiscuous_relay'). SI "la prueba falla[203]" ENTONCES Recomendar corregir esta situación.

3.3 Verificar que no exista FEATURE(`relay_based_on_MX'). SI "la prueba falla[204]" ENTONCES evaluar la necesidad de esta configuración y de no poder ser justificada Recomendar su eliminación.

3.4 Verificar que no exista FEATURE(`relay_local_from') SI "la prueba falla[205]" ENTONCES Recomendar corregir esta situación.

3.5 SI "el firewall no bloquea acceso desde el exterior" ENTONCES Verificar que no exista FEATURE(`accept_unresolvable_domains').

3.6 SI "la prueba falla[206]" ENTONCES Recomendar corregir esta situación.

3.7 Verificar que no exista FEATURE(`accept_unqualified_senders').SI "la prueba falla[207]" ENTONCES Recomendar corregir esta situación.

---

194 Redirecciones a programas no manejados oficialmente por el sistema, usuarios no conocidos por la organización, programas que no puedan garantizar la integridad de sus datos.etc..

195 Falla de la prueba significa que se han encontrado entra en /etc/aliases que no pueden ser justificadas.

196 Falla de la prueba significa que se han encontrado programas que pueden ser ejecutados por sendmail que no pueden ser justificados o que no superan las pruebas establecidas en la sección Programas Peligrosos.

197 No deben ser "escribibles" por el grupo o todo el mundo. El directorio tampoco

198 Falla de la prueba significa que se han encontrado archivos forward que pueden ser modificados por otros usuarios o cuyos dueños no corresponden con quien debe ser.

199 Revisar opción PrivacyOptions=restrctmailq,restrictqrun.

200 Falla de la prueba significa no se encuentra habilitada la opción 11.

201 El Relay por omisión está bloqueado, por esa razón la mayoría de las opciones posibles son para relajar los controles

202 Falla de la prueba significa que se puede hacer relay a dominios enteros.

203 Falla de la prueba significa que se encuentra habilitada la opción

204 Falla de la prueba significa qe se encuentra habilitada la opción sin justificación válida.

205 Falla de la prueba significa que se encuentra habilitada la opción

206 Falla de la prueba significa que se encuentra habilitada la opción lo cual implica que no se validan la existencia del dominio de quien envía.

207 Falla de la prueba significa que se encuentra habilitada la opción lo cual implica que no se solicitan los dominios de quien envía en el comando helo.

3.8 Verificar si existe FEATURE(`blacklist_recipients'). SI "la prueba falla[208]" ENTONCES Recomendar corregir esta situación.

3.9 Verificar si existe FEATURE(`dnsbl'). SI "la prueba falla[209]" ENTONCES Recomendar corregir esta situación.

4 PARA "Verificar existencia de servicios de autentificación"

4.1 Verificar si existe FEATURE(`STARTTLS'). SI "la prueba falla[210]" ENTONCES Recomendar corregir esta situación.

4.2 Verificar que exista la opción SMTP_AUTH. SI "la prueba falla[211]" ENTONCES Recomendar corregir esta situación.

4.3 Verificar que sendmail obligue la autentificación de los usuarios que envían email. SI "la prueba falla[212]" ENTONCES Recomendar corregir esta situación.

5 PARA "Verificar la efectividad y seguridad de las técnicas de prevención de ataques del tipo DoS"

5.1 Verificar opción MaxDaemonChildren. SI "la prueba falla[213]" ENTONCES Recomendar corregir esta situación.

5.2 Verificar opción MaxMessageSize. SI "la prueba falla[214]" ENTONCES Recomendar corregir esta situación.

5.3 Verificar max_connection_rate ,max_connections ,wait_for_client ,wait_for_server. SI "la prueba falla[215]" ENTONCES Recomendar corregir esta situación.

5.4 Verificar DelayLA. SI "la prueba falla[216]" ENTONCES Recomendar corregir esta situación.

5.5 Verificar MaxRecipientsMessage. SI "la prueba falla[217]" ENTONCES Recomendar corregir esta situación.

---

[208] Falla de la prueba significa que se no encuentra habilitada la opción lo cual implica que no chequea al remitente para verificar si ha sido declarado SPAM.

[209] Falla de la prueba significa que se no encuentra habilitada la opción lo cual implica que no chequea al remitente para verificar si ha sido declarado SPAM.

[210] Falla de la prueba significa que no se habilitan opciones adicionales de autentificación, en especial para el uso de PKI. Esto puede no ser un error si no existe ninguna PKI abierta con que validar los certificados que se presente,

[211] Falla de la prueba significa que no se habilitan opciones adicionales de autentificación, en especial permite definir procesos de autentificación mediante otros mecanismos tales como retos MD5, kerberos, etc...

[212] Falla de la prueba significa que no se habilitan opciones adicionales de autentificación para usuarios locales.

[213] Falla de la prueba significa el número de demonios que manejan sendmail no está de acuerdo al flujo real de mensajes del servidor.

[214] Falla de la prueba significa el tamaño máximo de los mensajes no está acorde a las necesidades de la organización.

[215] Falla de la prueba significa el los tiempos especificados pueden favorecer un ataque de DoS.

[216] Falla de la prueba significa el los tiempos especificados pueden favorecer un ataque de DoS.

[217] Falla de la prueba significa la cantidad de receptores de un mensaje definida pueden favorecer un ataque de DoS.

5.6 Verificar BadRcptThrottle. SI "la prueba falla[218]" ENTONCES Recomendar corregir esta situación.

6 PARA "Verificar la seguridad de otras opciones"

6.1 Verificar si no están activadas las opcionesVRFY y EXPN. SI "la prueba falla[219]" ENTONCES Recomendar corregir esta situación.

6.2 Verificar el nivel de bitácoras que se utiliza. SI "la prueba falla[220]" ENTONCES Recomendar corregir esta situación.

[218] Falla de la prueba significa la cantidad intentos de declarar usuarios de destino favorece un ataque de DoS o la enumeración de usuarios del sistema.

[219] Falla de la prueba significa que se solicitan estos comandos durante la conversación SMTP. Esto puede ser utilizado para realizar enumeración de usuarios.

[220] Falla de la prueba significa que se utiliza un nivel de logs inferior a 9.

Revisión de Servidores Apache.

Objetivo de esta sección: Realizar revisión de la configuración de servidores APACHE que afecten condiciones de riesgo de seguridad.
Durante esta revisión se buscan condiciones de riesgos que pudieron no ser develadas durante las pruebas de penetración.

Salida : Inventario de las vulnerabilidades encontradas y recomendaciones de solución.

DESARROLLO:

I. PARA "Revisar Servidores Apache" {
   A. Verificar la Seguridad de las condiciones generales de la instalación
   B. Verificar la Seguridad del ambiente de ejecución de CGI
   C. Verificar la Seguridad del esquema de protección general }

1 PARA "Verificar la Seguridad de las condiciones generales de la instalación"
1.1 Verificar SI "$ServerRootDirectory tiene permisos 511".
1.2 SI "prueba falla" ENTONCES Recomendar ajustar los permisos al valor establecido en la regla.
1.3 Verificar SI "$ServerRootDirectory es propiedad del root (root:root)".
1.4 SI "prueba falla" ENTONCES Recomendar ajustar la propiedad del subdirectorio al valor establecido en la regla.
1.5 Verificar SI " el ejecutable[221] del demonio es propiedad del root ".
1.6 SI "prueba falla" ENTONCES Recomendar ajustar la propiedad del subdirectorio al valor establecido en la regla.
1.7 SI "el servidor utiliza" SSI [222] ENTONCES Verificar SI la carga de CPU no se incrementa.[223]
1.7.1 SI "prueba falla[224]" ENTONCES Recomendar la evaluación de la necesidad del SSI.
1.7.2 SI "Usuarios pueden ejecutar CGI Propias o páginas con elementos SSI" ENTONCES Verificar que el wrapper suEXEC esté configurado[225].
1.7.2.1 SI "la prueba falla" ENTONCES Recomendar la habilitación y configuración del wrapper suEXEC.
1.7.2.2 Verificar que no está habilitado SSI. PARA archivos .html o .htm.
1.7.2.2.1.1 SI "la prueba falla[226]" ENTONCES Recomendar diferenciar las páginas que

[221] Revisar también el directorio que contiene al ejecutable.
[222] Server Side Include
[223] Para realizar esta prueba habrá que comparar la carga de CPU con el SSI habilitado y luego de haberlo deshabilitado.
[224] Falla de la prueba significa que hay un incremento significativo de la carga del CPU
[225] Debe estar configurado para usar un usuario diferente que el usado para correr el demonio httpd y que ese usuario no tenga permisos excesivos.
[226] Falla de la prueba significa que no se marquen diferenciadamente las páginas que posean elementos SSI.

usan SSI de las que no lo hacen.

2 PARA "Verificar la Seguridad del ambiente de ejecución de CGI"
  2.1 Verificar que los usuarios no pueden ejecutar programas CGI almacenados en cualquier directorio.
  2.2 SI "la prueba falla[227]" ENTONCES Recomendar revisar la politica de permisos para ejecutar CGI[228].
  2.3 SI "se permite ~/public_html/cgi-bin/ " ENTONCES verificar que los CGI no ponen en riesgo la seguridad (VER ANEXO PROGRAMA SEGURO) .
3 PARA "Verificar la Seguridad del esquema de protección general "
  3.1 Verificar que por omisión sólo se da acceso a los directorios correctos y se niega la resto.
  3.2 SI "la prueba falla[229]" ENTONCES Recomendar corregir inmediatamente la configuración.
  3.3 Verificar que Versión_actual =Versión_mas_actualizada.
  3.4 SI "la prueba falla[230]" ENTONCES Recomendar ctualizar servidor Apache.
  3.5 SI "SI se utiliza control de acceso[231]" ENTONCES Verificar fortalezas de las contraseñas[232]
    3.5.1 SI "la prueba falla[233]" ENTONCES Recomendar revisar la politica de contraseñas.
    3.5.2 Verificar permisos del archivo htaccess.
    3.5.3 SI "la prueba falla[234]" ENTONCES Recomendar revisar la politica de permisos
    3.5.4 Verificar que los permisos de los archivos .htaccess no sobreescriban los permisos generales del servidor.[235]
    3.5.5 SI "la prueba falla[236]" ENTONCES Recomendar revisar la de permisos para evitar esta situación
  3.6 SI se permite public_html ENTONCES Verificar permisos de archivos.
    3.6.1 SI "la prueba falla[237]" ENTONCES Recomendar revisar la politica de permisos
  3.7 SI EXISTE Usuario_del_demonio ENTONCES Verificar que no tenga shell válido.
    3.7.1 SI "la prueba falla[238]" ENTONCES Recomendar cambiar el shell a no válido.
    3.7.2 Verificar que no tenga home válido.
    3.7.3 SI "la prueba falla[239]" ENTONCES Recomendar borrar el directorio $HOME no existente.

[227] Falla de la prueba significa que los usuarios pueden ejecutar CGI en cualquier directorio.
[228] Esta opción deberá depender del nivle de confianza que se posea en los usuarios. Por omisión no se recomienda permitir.
[229] Falla de la prueba significa que los usuarios pueden ejecutar CGI en cualquier directorio.
[230] Falla de la prueba significa que los usuarios pueden moverse con libertad por toda la estructura del sistema de archivos del servidor
[231] Se refiere a control a través de medios como los archivos .htaccess ó equivalentes.
[232] Ver sección de pruebas de penetración
[233] Falla de la prueba significa que se logran descifrar a menos una contraseña.
[234] Falla de la prueba significa que los permisos permiten que cualquier usuario modifique (borre) el archivo .htaccess
[235] Verificar AllowOverride None
[236] Falla de la prueba significa que los permisos permiten que cualquier usuario modifique los permisos dados al servidor.
[237] Falla de la prueba significa que los permisos permiten que cualquier usuario modifique (borre) el archivo directorio public_html.
[238] Falla de la prueba significa que el usuario con que corre el demonio tiene en /etc/passwd un shell que permite a un usuario tomar su identidad y ejecutar comandos.
[239] Falla de la prueba significa que el usuario con que corre el demonio tiene en /etc/passwd un sudbirectorio $HOME existente. Valido para nota 18 y 19 -> $HOME: /dev/null /$SHELL: sbin/nologin

3.7.4 Verificar que el servicio se ejecute bajo el usuario root.
3.7.5 SI "la prueba falla" ENTONCES Recomendar inmediatamente cambiar usuario con que se ejecuta el demonio.
3.7.6 Verificar que sólo se entrege la información necesaria sobre el servidor[240].
3.7.7 SI "la prueba falla" ENTONCES Recomendar inmediatamente cambiar el valor de configuración.
3.7.8 Verificar que existan y se mantengan bitácoras del servidor.
3.7.9 SI "la prueba falla"[241] ENTONCES Recomendar inmediatamente cambiar el valor de configuración.

[240] Verficar ServerSignature Off ServerTokens Prod=off.
[241] Falla en la prueba significa que no se encuentren bitácoras.

Revisión de la Infraestructura Inalámbrica

Objetivo de esta sección: Realizar revisión de la configuración de los sistemas inálambricos
Durante esta revisión se buscan condiciones de riesgos que pudieron no ser develadas durante las pruebas de penetración.

Salida : Inventario de las vulnerabilidades encontradas y recomendaciones de solución.

DESARROLLO:

I. PARA "Revisar la Seguridad de la Infraestructura Inalámbrica" {
   A. Verificar la seguridad del esquema de autentificación y control de acceso
   B. Verificar la seguridad del sistema DHCP
   C. Verificar los mecanismos de control de integridad y confidencialidad
   D. Verificar la Seguridad del entorno }

1 PARA "Verificar la seguridad del esquema de autentificación y control de acceso"

1.1 Verificar si se divulga el SSID por broadcast .

1.2 SI "la prueba falla[242]" ENTONCES Recomendar inhabilitar esta configuración

1.3 Verificar que no se utilicen los SSID por omisión .

1.4 SI "la prueba falla[243]" ENTONCES Recomendar inhabilitar esta configuración

1.5 PARA "cada dispositivo de acceso inalámbrico"Verificar si hay control de acceso por direcciones MAC.

1.5.1 SI "la prueba falla[244]" ENTONCES Verificar si este tipo de control de acceso es válido para el ambiente que se evalúa.

1.5.1.1 SI "la prueba falla[245]" ENTONCES Recomendar que se active este tipo de control.

1.6 Verificar si se ha implantado 802.1i para el ambiente.

1.6.1 SI "la prueba falla[246]" ENTONCES Recomendar habilitar esta configuración

1.6.2 Si "la prueba no falla" ENTONCES SI "se utilizan contraseñas locales" ENTONCES

[242] Falla de la prueba significa que uno o más puntos de acceso radian su SSID a cualquier estación.
[243] Falla de la prueba significa que uno o más puntos de acceso utilizan el SSID del fabricante por omisión.
[244] Falla de la prueba significa que uno o más puntos de acceso utilizan el SSID del fabricante por omisión.
[245] Falla de la prueba implica que es factible el control de acceso por direcciones MAC
[246] Falla de la prueba significa no existe una arquitectura de autentifiación

Verificar si se utilizan contraseñas seguras.

1.6.2.1.1 SI "la prueba falla[247]" ENTONCES Recomendar urgentemente aumentar el nivel de seguridad de las contraseñas.

1.6.2.1.2 Verificar si se utilizan contraseñas de cambios periódicos.

1.6.2.1.3 SI "la prueba falla" ENTONCES Recomendar utilizar contraseñas periódicas

1.6.2.2 SI "se utiliza secreto compartido" ENTONCES Verificar si las contraseñas son robustas.

1.6.2.2.1 SI "la prueba falla[248]" ENTONCES Recomendar urgentemente aumentar el nivel de seguridad de las contraseñas.

2 PARA " Verificar la seguridad del sistema DHCP"

2.1 Si "se utiliza DHCP" ENTONCES Verificar que las opciones del ámbito DHCP no divulgue información de la red.

2.1.1.1 SI "la prueba falla[249]" ENTONCES Recomendar redefinir las opciones de DHCP Verificar que los tiempos de asignación de configuración sean los correctos.

2.1.1.2 SI "la prueba falla[250]" ENTONCES Recomendar reconfigurar está opción.

3 PARA "Verificar los mecanismos de control de integridad y confidencialidad"

3.1 Verificar si se utiliza algún esquema de cifrado.

3.1.1 SI se utiliza WEP ENTONCES Verificar si se utiliza TKIP.

3.1.1.1 SI "la prueba falla[251]" ENTONCES Recomendar el uso de TKIP.

3.1.2 Verificar si se utiliza WPA ó WPA2.

3.1.2.1 SI "la prueba falla[252]" ENTONCES Recomendar el uso de WPA (1 ó 2).

3.2 Verifica que los usuarios no pueden elegir modos de trasmisión inseguros.

3.2.1 SI "la prueba falla[253]" ENTONCES Recomendar urgentemente corregir cualquier configuración que permita a los usuarios utilizar modos no seguros (planos) de transmisión.

4 PARA "Verificar la Seguridad del entorno"

[247] Falla de la prueba significa que las contraseñas son inseguras (triviales, sencillas, fácilmente rompibles.

[248] Falla de la prueba significa que las contraseñas son inseguras (triviales, sencillas, fácilmente rompibles.

[249] Falla de la prueba significa que uno o más puntos de acceso otorgan configuraciones por DHCP que de

[250] Falla de la prueba significa que los tiempos de entrega de las configuraciones IP exceden los valores recomendados para la arquitectura que se analiza.

[251] Falla de la prueba significa que al menos uno de los dispositivos involucrados en la red inalámbrica no utilizan TKIP lo que hace al esquema de cifrado vulnerable.

[252] Incluso si se utiliza WEP debe valorarse la opción de escalar a WPA.

[253] Falla de la prueba significa que al menos uno de los puntos de acceso que forman la red permite el acceso no seguro a la misma.

4.1 Verificar si los puntos de acceso inalámbricos son accesibles desde fuera de la organización.

4.1.1 SI "la prueba falla[254]" ENTONCES Recomendar corregir la configuración para evitar conexiones desde el exterior.

4.2 Verificar que las reglas de filtrado que se aplican a la red inalámbrica[255]

4.2.1 SI "la prueba falla[256]" ENTONCES Recomendar corregir la política de filtrado para incluir a la red inalámbrica.

4.3 Verificar que las reglas detección de intrusos que se aplican a la red inalámbrica[257]

4.3.1 SI "la prueba falla[258]" ENTONCES Recomendar corregir la política de filtrado para incluir a la red inalámbrica.

[254] Falla de la prueba significa que se puede acceder y conectar desde afuera
[255] Ver sección de chequeo de firewalls para verificar estás reglas con las que se aplican a la red inalámbrica.
[256] Falla de la prueba significa que la red inalámbrica se encuentra desprotegida.
[257] Ver sección de chequeo de IDS para verificar estás reglas con las que se aplican a la red inalámbrica.
[258] Falla de la prueba significa que no se hace chequeo de intrusos en la red inalámbrica.

Revisión de Sistemas de Detección de Intrusos.

Objetivo de esta sección: Realizar revisión de la configuración de los sistemas de detección de intrusos basados en red y hosts
Durante esta revisión se buscan condiciones de riesgos que pudieron no ser develadas durante las pruebas de penetración.

Salida : Inventario de las vulnerabilidades encontradas y recomendaciones de solución.

DESARROLLO:

I. PARA "Revisar la Seguridad los Sistemas de Detección de Intrusos" {
   A. Verificar la configuración básica de seguridad de un Detector de Intrusos Basado en red (NDIS)
   B. Verificar la seguridad del sistema los Sistemas de Detección de Intrusos basados en host}

1. PARA "Verificar la configuración básica de seguridad de un Detector de Intrusos Basado en red (NDIS)"

1.1 SI "los NDIS generan alarmas" ENTONCES Verificar niveles de alerta y atención de las alarmas[259] DE LO CONTRARIO Recomendar ajuste de los niveles de alertas.
1.2 SI "Existen Alertas pero no son correctos sus niveles" ENTONCES Recomendar ajuste de los niveles de alertas.
1.3 SI "Existen firmas nuevas"ENTONCES verificar la distribución de las firmas pasadas 5 m, 12 h y 24 h .
1.3.1.SI "las alertas no se han difundido en a lo sumo en 24 h" ENTONCES Recomendar Ajuste y verificación del sistema de actualización de firmas.
1.4 Generando tráfico pseudo-hostil[260], y que pueda ser detectado por el NDIS
1.4.1.SI "las bitácoras del NDIS se llenan" ENTONCES
1.4.1.1. SI "el desbordamiento de las bitácoras ocurrió debido a poco espacio en las mismas" ENTONCES Recomendar ampliación del tamaño de las bitácoras incluyendo la posibilidad de centralización y trasmisión segura de las mismas.
1.4.1.2. SI "el desbordamiento de las bitácoras ocurrió debido a exceso de alertas registradas" ENTONCES Recomendar ajuste de los niveles de Registro de Alertas e Incidentes.
1.4.2. Verificar que la información almacenada en las bitácoras sea correcta y completa para reconocer efectivamente un ataque [261]

[259] A quien le llegan, que información, por que medios y en que tiempo.
[260] Tráfico generado con un programa de búsqueda automática de vulnerabilidades
[261] Reconocer un ataque significa: Origen Real, Objetivo del ataque, método utilizado

1.4.3.SI "la prueba falla[262]" ENTONCES Recomendar Ajuste de los niveles de Registro del NDIS

1.4.4. SI NDIS es Activo ENTONCES Verificar que las acciones provocadas por los mandatos del NDIS sean adecuadas[263] DE LO CONTRARIO Recomendar ajustes en el tipo de acciones del NDIS.

1.5 Genera tráfico hostil [264]

1.5.1.SI "NDIS no es capaz de detectar tráfico con variaciones de la taza de envíos" ENTONCES Recomendar ajustes en las firmas del NDIS.

1.5.2.SI "NDIS no es capaz de detectar cambios en las direcciones IP de origen (spoofing)" ENTONCES Recomendar ajustes en las firmas del NDIS.

1.5.3.SI "NDIS no es capaz de detectar ataques encapsulados en otros protocolos" ENTONCES Recomendar ajustes en las firmas del NDIS.

1.6 Revisar las bitácoras de los NDIS

1.6.1. Verificar si se han registrado las acciones realizadas por las pruebas.

1.6.2.SI "la prueba falla[265]" ENTONCES Tratar de encontrar la razón del error y Recomendar ajustes.

1.7 Verificar si el NDIS cubre todos los sitios en la red donde es importante que se capture tráfico.

1.7.1.SI "la prueba falla[266]" ENTONCES Recomendar Rediseño del la arquitectura de monitoreo para tomar en cuenta todos los puntos críticos.

1.8 Verificar si en cada punto de captura de datos se captura la información completa.

1.9 SI "la prueba falla[267]" ENTONCES Recomendar ajuste de los mirror o taps de los puntos de captura de información

2. SI "Existen IDS Basados en Hosts"[268] ENTONCES Verificar si todos los servidores críticos posean IDS.

2.1 SI "la prueba falla[269]" ENTONCES Recomendar la ampliación de la plataforma de IDS para que cubra todos los Servidores.

2.2 Verificar que " todos los servicios críticos posean IDS".

2.2.1.SI "la prueba falla[270]" ENTONCES Recomendar la ampliación de la plataforma de IDS para que cubra todos los Servicios.

2.3 Verificar si la información guardada en las bitácoras de los servidores permite el funcionamiento adecuado de los IDS.

2.3.1.SI "la prueba falla[271]" ENTONCES Recomendar mejoras en el sistemas de bitácoras[272].

---

[262] La falla de la prueba implica que la información guardada en las bitácoras no es suficiente para definir un rastro del atacante y la forma en que se realizó el ataque.

[263] Adecuadas significa: Eliminen o minimicen el ataque sin poner en riesgo o paralizar otras operaciones

[264] Tráfico generado con firmas especificas de ataques según el tipo de los mismos

[265] Falla de la prueba implica que no se han registrado los ataques realizados.

[266] Falla de la prueba implica que no se revisan todos los sitios importantes de la red.

[267] Falla de la prueba implica que la información que se captura no es completa.

[268] A efecto de este documento se nombrarán simplemente IDS. En las secciones revisión de servidores Unix y Revisión de servidores Windows se ha revisando en profundidad este punto .

[269] Falla de la prueba implica que no se revisan todos los servidores importantes de la red.

[270] Falla de la prueba implica que no se revisan todos los servicios importantes de la red.

[271] Falla de la prueba implica que con la información guardada el IDS no puede detectar posibles ataques

[272] Syslog o equivalente

2.4 SI Existen servicios de rotación de bitácoras ENTONCES
  2.4.1. Verificar si no interfieren con el funcionamiento del IDS.
  2.4.2. SI "la prueba falla[273]" ENTONCES Recomendar ajustes en la política de rotación de bitácoras

[273] Falla de la prueba implica que la rotación de bitácoras impide el funcionamiento correcto del IDS.

Revisión de Dispositivos Firewalls

Objetivo de esta sección: Realizar revisión de la configuración de dispositivos firewalls de red.
Durante esta revisión se buscan condiciones de riesgos que pudieron no ser develadas durante las pruebas de penetración.

Salida : Inventario de las vulnerabilidades encontradas y recomendaciones de solución.

DESARROLLO:

I. PARA "Revisar la Seguridad los Sistemas de Detección de Intrusos" {
   A. Verificar efectividad de las reglas de filtrado
   B. Verificar efectividad de las políticas de mantenimiento de la configuración
   C. Verificar configuración y seguridad del sistema de bitácoras }

1 PARA "Verificar efectividad de las reglas de filtrado"
1.1 Verificar que las reglas de filtrado del firewall sigan el siguiente orden:
   1. Filtros anti spoofing[274] (blocked private addresses, internal addresses appearing from the outside
   2. Reglas permisivas de los usuarios.
   3. Reglas para el manejo de la infraestructura.
   4. Descarga de protocolos[275]
   5. Reglas de bloqueo y alerta
   6. Reglas de bloqueo y almacenamiento en bitácoras.

   1.1.1 SI "la prueba falla[276]" ENTONCES Recomendar ajustar política de filtrado para ejecutarse según el orden que se ha señalado

1.2 Verificar que las reglas sean adecuadamente establecidas en función de IP de origen y destino, puertos de origen y destino y tiempos máximos de espera (timeouts).
   1.2.1 SI "la prueba falla[277]" ENTONCES Recomendar ajustar política de filtrado .

1.3 Verificar que las reglas de filtrado existen en ambos sentidos para cada una de las interfaces con que cuente el firewall.
   1.3.1 SI "la prueba falla[278]" ENTONCES Recomendar ajustar política de filtrado para filtrar en ambos sentidos el tráfico no permitido.

[274] Bloqueo de direcciones internas que aparecen en la zona externa o viceversa
[275] Ej. Paquetes OSPF, transferencias de zona. etc.
[276] Falla de la prueba implica errores en la política de filtrado, temas no tomados en cuenta, cambio de la política por omisión, etc.
[277] Falla de la prueba implica errores en la política de filtrado que implique relajamiento de las reglas.
[278] Falla de la prueba implica errores en la política de filtrado que no cierran en ambos sentidos el tráfico no permitido. Esto favorece ataques del tipo black-end

1.4 Verificar la existencia de zona definidas por el firewall.
1.4.1 SI "la prueba falla[279]" ENTONCES Recomendar ajustar política de filtrado para crear zonas diferentes en función del tipo de acceso que deben tener cada una.
1.5 Verificar que las direcciones definidas en RFC 1918 está bloqueadas (VER ANEXO FIREWALLS-1) desde el exterior a el resto de las zonas.
1.5.1 SI "la prueba falla[280]" ENTONCES Recomendar ajustar política filtrado.
1.6 Verificar que los puertos que se enumeran en ANEXO FIREWALLS-2 son bloqueados desde la zona externa hacia la zona interna[281].
1.6.1 SI "la prueba falla[282]" ENTONCES Recomendar ajustar política de filtrado para filtrar los puertos que se mencionan.
1.7 Verificar que existan reglas de filtrado para el tráfico ICMP tipo 8, 11, 3.
1.7.1 SI "la prueba falla[283]" ENTONCES Recomendar ajustar política de filtrado para filtrar tipos de servicios ICMP que se mencionan.
1.8 Verificar si el firewall es stateful.
1.8.1 SI "la prueba falla[284]" ENTONCES Recomendar ajustar política de filtrado para evitar que el firewall acepte conexiones no establecidas a través de él.
1.9 SI "existen reglas de redirección" ENTONCES Verificar que las direcciones internas no son mostradas en el exterior.
1.9.1 SI "la prueba falla[285]" ENTONCES Recomendar ajustar política de filtrado para evitar esta situación.
1.10 Verificar que sólo se permite tráfico generado en la zona interna[286].
1.10.1 SI "la prueba falla[287]" ENTONCES Recomendar ajustar política de filtrado para impedir que se permita tráfico servidor hacia la zona interna.
1.11 Verificar que explícitamente se niega todo tráfico desde la zona externa hacia los servidores críticos que se encuentren en la zona interna.
1.11.1 SI "la prueba falla[288]" ENTONCES Recomendar ajustar política de filtrado para impedir que se permita hacia los servidores que se encuentren en la zona interna y que sean críticos.
2 PARA "Verificar efectividad de las políticas de mantenimiento de la configuración de los firewalls"
2.1 Verificar si existen políticas de mantenimiento de la configuración del firewall.
2.2 SI "la prueba falla[289]" ENTONCES Recomendar crear una política de mantenimiento de la

[279] Falla de la prueba implica la inexistencia de alguna de las zonas mínimas (externa-DMZ-interna)
[280] Falla de la prueba implica incumplimiento de la RFC.
[281] Si la política por omisión es la correcta estos puertos están implícitamente cerrados.
[282] Falla de la prueba implica que alguno de los puertos que se menciona se mantienen abiertos sin justificación de uso.
[283] Falla de la prueba implica que alguno de los tipos de servicio ICMP se permiten que pasen desde el exterior hacia cualquiera de las zonas.
[284] Falla de la prueba implica que el firewall no cheque al bit de ACK de las conexiones TCP o recuerda las conexiones en el caso del UDP. Posiblemente esta condición implique la recomendación de cambio del firewall.
[285] Falla de la prueba implica que las direcciones de la red interna son anunciadas al exterior.
[286] Se refiere impedir tráfico generado en la zona externa o DMZ y cuyo destino sea la zona interna.
[287] Falla de la prueba implica la posibilidad de acceder a máquinas en la zona interna que den algún servicio.
[288] Falla de la prueba implica la posibilidad de acceder a servidores críticos que se encuentren en la zona interna desde el exterior.
[289] Falla de la prueba implica la inexistencia de políticas de respaldo, actualización, reajuste de las reglas de filtrado.

configuración del firewall.

3 PARA "Verificar configuración y seguridad del sistema de bitácoras¨

3.1 Verificar si existen bitácoras del funcionamiento del firewall y de las aplicaciones de las reglas de filtrado.

3.1.1 SI "la prueba falla[290]" ENTONCES Recomendar crear urgentemente una política de bitácoras.

[290] Falla de la prueba implica la inexistencia de políticas de bitácoras del funcionamiento del firewall.

Revisión de las Políticas de Seguridad

Objetivo de esta sección: Realizar revisión de la configuración de las política de seguridad existentes en la empresa (establecidas formalmente y de facto). Durante esta revisión se buscan condiciones de riesgos que pudieron no ser devaladas durante las pruebas de penetración.

Salida : Inventario completo los aspectos que cubre la política de seguridad (si existe) y aquellos elementos que no son tomados en cuenta por la política.

La evaluación está basada en las recomendaciones del ISO 17799, el cual posee 10 capítulos:

CAP 1 De la Propia Política de Seguridad

CAP 2 Seguridad Organizacional

CAP 3 Clasificación y Control de Activos

CAP 4 Seguridad Personal

CAP 5 Seguridad Física y Ambiental

CAP 6 Gestión de Operaciones y Comunicaciones

CAP 7 Control de Acceso

CAP 8 Desarrollo y Mantenimiento de Sistemas

CAP 9 Gestión de la Continuidad de Negocio

CAP 10 Cumplimiento del Marco Jurídico

DESARROLLO:

I. PARA "Revisar la Seguridad los Sistemas de Detección de Intrusos" {
   A. Verificar el cumplimiento de los objetivos del Cap 1 ISO17799
   B. Verificar el cumplimiento de los objetivos del Cap 2 ISO17799
   C. Verificar el cumplimiento de los objetivos del Cap. 3, ISO17799
   D. Verificar el cumplimiento de los objetivos del Cap 4 ISO17799
   E. Verificar el cumplimiento de los objetivos del Cap. 5 ISO17799
   F. Verificar el cumplimiento de los objetivos del Cap 6 ISO17799
   G. Verificar el cumplimiento de los objetivos del Cap 7 ISO17799

H. Verificar el cumplimiento de los objetivos del Cap 8 ISO17799"

I. Verificar el cumplimiento de los objetivos del Cap. 9 ISO17799

J. Verificar el cumplimiento de los objetivos del Cap 10 ISO17799 }

1. PARA "Verificar el cumplimiento de los objetivos del Cap. 1 ISO17799"

1.1 Verificar si la Gerencia conoce y apoya la política de seguridad (PS) establecida

1.2 Verificar que la política esté correctamente almacenada y esté disponible para los miembros de la organización.

1.3 Verificar que la política de seguridad es conocida por los miembros de la organización.

1.4 Verificar que la PS incluye una declaración de:

- Apego a la normativa legal y requerimientos vigentes
- Requerimientos de educación en seguridad
- Uso indebido de los activos de información
- Acceso al sistema
- Prevención y detección de software malicioso
- Gestión de la continuidad del negocio
- Consecuencias y sanciones de las violaciones a las políticas de seguridad
- Una definición especificando las responsabilidades generales y específicas por la gestión de la seguridad de la información, incluyendo el reporte de incidentes de seguridad.
- Una definición especificando las responsabilidades generales y específicas por la gestión de la seguridad de la información, incluyendo el reporte de incidentes de seguridad.
- Definición de Responsabilidades

1.4.1 SI "La Prueba Falla[291]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

2 PARA "Verificar el cumplimiento de los objetivos del Cap. 2, ISO17799"

[291] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 1 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

2.1 Verificar que la política establece la manera de:

- Establece un foro de gestión de seguridad de la información
- Define y delimita roles y responsabilidades en cuanto a la seguridad de la información
- Establece procedimientos de autorización para la adopción de facilidades de procesamiento de información
- Designa un consejero especialista en seguridad de la información
- Promueve la cooperación entre organizaciones
- Asegura la revisión independiente o externa de la implementación de las políticas de seguridad de la información.

2.1.1 SI "La Prueba Falla[292]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

3 PARA "Verificar el cumplimiento de los objetivos del Cap. 3, ISO17799"

3.1 Verificar que la política establece la manera de:

- Mantener una protección adecuada de los activos de la organización
- Asegurar que los activos de información reciben un nivel apropiado de protección.

3.1.1 SI "La Prueba Falla[293]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

4 PARA "Verificar el cumplimiento de los objetivos del Cap. 4 ISO17799"

4.1 Verificar que la política establece la manera de :

- Reducir los riesgos de error humano, hurto, fraude o mal uso de las facilidades que procesan información.
- Asegurar que los usuarios son conscientes de las amenazas a la seguridad de la información, que deben involucrarse en su protección y que son preparados y equipados para cumplir con la política de seguridad corporativa dentro de sus actividades diarias en el trabajo.
- Minimizar el daño provocado por incidentes de seguridad o por mal funcionamiento de los sistemas y aprender de tales incidentes.

[292] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 2 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

[293] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 3 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

4.1.1 SI "La Prueba Falla[294]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

5 PARA "Verificar el cumplimiento de los objetivos del Cap. 5 ISO17799"

5.1 Verificar que la política establece la manera de:

- Prevenir accesos no autorizados, daños e interferencias a las posesiones y activos de la organización.
- Prevenir pérdida, daño o compromiso a los activos de información y la interrupción de las actividades del negocio.
- Prevenir el compromiso o robo de la información y de las facilidades de procesamiento de la información.

5.1.1 SI "La Prueba Falla[295]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

6 PARA "Verificar el cumplimiento de los objetivos del Cap. 6 ISO17799"

6.1 Verificar que la política establece la manera de:

- Asegurar la operación correcta y segura de las facilidades de procesamiento de información
- Minimizar el riesgo de falla del sistema
- Proteger la integridad del software y de la información
- Mantener la integridad y disponibilidad de los servicios de procesamiento de la información y comunicación
- Asegurar la protección de la información dentro de ambientes de redes y de su infraestructura de soporte
- Prevenir daño a los activos de información y la interrupción de las actividades del negocio
- Prevenir pérdida, modificación o manejo inadecuado de la información intercambiada entre organizaciones

6.1.1 SI "La Prueba Falla[296]" ENTONCES Recomendar corregir los aspectos deficientes

[294] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 4 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

[295] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 5 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

[296] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 6 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

7 PARA "Verificar el cumplimiento de los objetivos del Cap. 7 ISO17799"

7.1 Verificar que la política establece la manera de:

- Controlar el acceso a la información
- Prevenir accesos no autorizados a los sistemas de información
- Prevenir accesos de usuarios no autorizados
- Asegurar la protección de servicios de red
- Prevenir accesos no autorizados a los equipos de cómputo
- Detectar actividades no autorizadas
- Asegurar la seguridad de la información cuando se empleen facilidades de computación móvil y tele-trabajo.

7.1.1 SI "La Prueba Falla[297]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

8 PARA "Verificar el cumplimiento de los objetivos del Cap. 8 ISO17799"

8.1 Verificar que la política de seguridad establece como:

- Asegurar que la seguridad esté incluida como requerimiento dentro los sistemas en operación
- Prevenir la pérdida, modificación o mal uso de los datos de los usuarios dentro de las aplicaciones
- Garantizar la confidencialidad, autenticidad e integridad de la información
- Asegurar que los proyectos de tecnologías de la información y actividades de soporte son conducidas en una manera segura
- Mantener la seguridad del software de las aplicaciones y sus datos.

8.1.1 SI "La Prueba Falla[298]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

9 PARA "Verificar el cumplimiento de los objetivos del Cap. 9 ISO17799"

9.1 Verificar que la política de seguridad establece como:

[297] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 7 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

[298] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 8 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

- Identificar y priorizar los procesos críticos del negocio de acuerdo a su impacto en la continuidad del negocio
- Considerar la adquisición de un seguro contra siniestros adecuado
- Formular y documentar una estrategia de continuidad del negocio basada en los objetivos y prioridades del negocio
- Formular y documentar planes de contingencia en concordancia con la estrategia acordada
- Realizar pruebas periódicas y ajustes de los planes y procesos formulados
- Asegurar que la gestión de la continuidad del negocio forme parte de la estructura y procesos de la organización

9.1.1 SI "La Prueba Falla[299]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

10 PARA "Verificar el cumplimiento de los objetivos del Cap. 10 ISO17799"

10.1 Verificar que la política de seguridad establece como:

- Asegurar que los sistemas cumplen con las políticas y estándares de seguridad de la organización
- Maximizar la efectividad y minimizar la interferencia en los procesos de auditoría de los sistemas

10.1.1 SI "La Prueba Falla[300]" ENTONCES Recomendar corregir los aspectos deficientes detectados en la política de seguridad ó en la forma en que esta es aplicada en la organización bajo prueba.

FIN DE LAS REGLAS QUE CONTITUYEN EL MODELO.

[299] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 9 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

[300] Falla de la Prueba significa que alguno de los elementos definidos por el Cap. 10 del ISO 17799 no ha sido correctamente abordado en la política existente o simplemente ha sido pasado por alto en la misma.

Capítulo 4. Validación Práctica del Modelo

En este capítulo describiremos las pruebas y análisis realizados para la validación del modelo. Primeramente se mostrará una comparación entre el modelo propuesto en trabajo y el conjunto de pruebas que se ejecutan actualmente. Posteriormente mostraremos los resultados obtenidos durante un proceso de auditoría utilizando el modelo que proponemos.

1. Comparación con el esquema actual

El modelo propuesto fue comparado con el conjunto de pruebas utilizado actualmente para auditar. La primera gran diferencia es que actualmente no se utiliza un modelo normalizado sino un conjunto empírico de pruebas que se siguen sin un orden establecido e incluso cambian de vez en vez que se ejecuta una auditoría, lo cual dificulta enormemente la comparación del estado (evolución o involución) de un sitio luego de haber sido auditado más de una vez. Igualmente sucede con las recomendaciones.

La segunda gran diferencia es cualitativa tal y como muestra la siguiente tabla (tabla 2) el número de pruebas se ha incrementado de manera significativa (355 %). Un elemento importante para comprender el significado real de este incremento es entender como han sido seleccionadas las pruebas que constituyen el modelo propuesto: la selección de pruebas fue realizada tomando en cuenta las necesidades reales de RedULA (las cuales no deben diferir significativamente de las necesidades de cualquier entidad de su tipo, debido a la similitud de arquitectura, tecnologías, actores y riesgos). No se trata solo de incremento del número de pruebas sino de una selección cuidadosamente realizada en las primeras etapas de concepción del modelo, para asegurar que el mismo responda a las necesidades y características del sitio donde será principalmente utilizado.

	Cantidad de Pruebas		
Categoría	Modelo Propuesto	Esquema Actual	% de Incremento de la cantidad de Pruebas
Pruebas de Penetración	82	36	227,78%
Seguridad Física	9	1	900,00%
Revisión de Servidores Unix	61	17	358,82%
Revisión de Servidores y Estaciones Windows	69	7	985,71%
Revisión de Servidores Apache	19	4	475,00%
Revisión de Servidores Sendmail	28	10	280,00%
Revisión de la Infraestructura Inalámbrica	15	6	250,00%
Revisión del Sistema de Detección de Intrusos	18	6	300,00%
Revisión de Dispositivos Firewalls	13	5	260,00%
Revisión de las Políticas de Seguridad	55	12	458,33%
TOTALES	**369**	**104**	**354,81%**

Tabla 2: Comparación cuantitativa entre la cantidad de controles del modelo propuesto y de que se aplica actualmente

2. Pruebas del Modelo

Tal y como fue declarado en la propuesta que dio origen a este trabajo, el modelo fue probado para corregir los detalles que el criterio verificador de la práctica indicase: incorporar elementos que pudiesen haber sido pasados por alto o eliminar aquellos que no fuese práctico ejecutar en la práctica cotidiana de auditoría o en alguna circunstancia particular.

Tomando en cuenta el carácter público de este documento y la necesaria privacidad y protección de los

datos emanados del proceso de auditoría, se ha tomado la decisión de proteger todo aquella información que pudiese develar datos críticos del sitio auditado. La protección se ha establecido de la siguiente forma:

- Las direcciones IP, públicas y privadas[301], ha sido cambiadas.
- Los dominios han sido modificados a fin de no ser reconocibles.
- Los nombres de máquinas, tanto de servidores como de estaciones, han sido modificados
- Los nombres y direcciones IP de los sitios con los que establece conexiones el sitio auditado han sido modificados.
- El nombre, personal, localización física y proveedores de servicios han sido modificados.

1 Arquitectura del sitio Auditado.

La dependencia escogida para hacer la prueba del modelo solicitó, debido a serias dudas sobre el estado de la seguridad de su plataforma de IT realizar una auditoría de la seguridad de sus sistemas y la posterior corrección de las condiciones de riesgo encontradas, a fin de poder para poder ejecutar una rigurosa planificación de capacidades y crecimiento.

Como resultado de la ejecución del módulo 1 se determinó que el equipo auditor estaría formado por 2 personas, las cuales realizarían conjuntamente los módulos Pruebas de Penetración y Revisiones. Se determinó adicionalmente que el tiempo para ejecutar las pruebas y revisiones sería de 1 semana, por último se escogieron a los contactos de ambas partes y se determinó el alcance del ejercicio de la siguiente manera: Se debían auditar todos los servicios que se ofrecen, fuesen visibles o no desde el exterior, debería auditarse además 5 máquinas clientes. En el proceso de auditoría se debería incluir a los dispositivos de comunicaciones y seguridad existentes.

No se planificaron pruebas de robo de información en la red (fisgoneo).

Como resultado la la ejecución del módulo 2 se obtuvieron los siguientes resultados:

- Rango de direcciones privadas: 192.168.123.0 /24
- Rango de direcciones públicas: 150.189.200.225/29
- Cantidad de Servidores de Correo: 1
    - Demonio de Correo: Sendmail

[301] En teoría las direcciones privadas pudiesen ser divulgadas sin mayor peligro. Sin embargo, errores en la configuración de los servicios de nombres permiten encontrar direcciones de las zonas privadas haciendo requerimientos normales de DNS. Esa situación crítica ha sido corregida gracias al proceso de auditoría.

    - Sistema Operativo del Servidor: RedHat 9.0
- Servidores WEB: 1
    - Demonio Web: Apache 1
    - Sistema Operativo del Servidor: Windows 2000
- Otros Servicios: DNS: Bind v. 4.9.11
- Otros Servicios: Web Mail : Squirrelmail 1.4.5
- Otros Servicios: Alojamiento de cuentas. Las cuentas se encuentran alojadas en el propio servidor de correo.
- Otros Servidores: Web (apache 1 sobre Windows 2000) para pruebas de sistema de gestión
- Servicios de Seguridad: Cortafuegos Marca WatchGuard y consola de administración del equipo en Windows 2000.

El sitio auditado tenía una arquitectura similar a la que se indica en la figura siguiente.

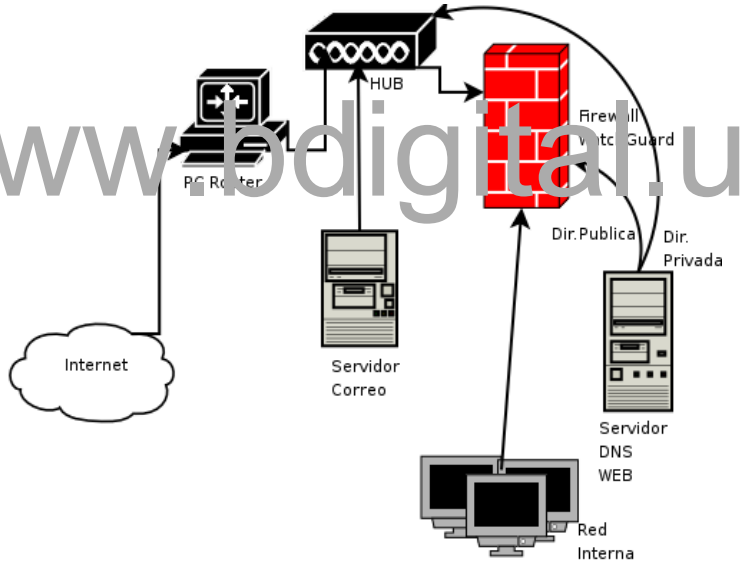


Ilustración 6: Esquema de la arquitectura de redes del sitio auditado con el modelo propuesto

2 Resultados de la Ejecución del Módulo 3: Pruebas de Penetración

A continuación se destacan los resultados más significativos de las pruebas realizadas. Se han resumido los resultados entendiéndose que el objetivo de su presentación es demostrar la correctitud del modelo de auditoría. Se han dividido los resultados por secciones, siguiendo estrictamente el orden en el que aparecen en el modelo. Los resultados se presentan resumidos en siguiente tabla Junto a cada hallazgo se establece mediante que prueba(s) del modelo, fue obtenido. En la sección 2.1 se muestran algunas evidencias recabadas durante la ejecución de las pruebas de penetración.

Sección	Hallazgos
Definir la arquitectura sin conocimiento	1- Se identificaron los puntos de acceso al exterior, pudiéndose identificar la marca de los equipos, sistema operativo, saltos de las rutas (Prueba 1.1) 2- Se reconoció todo el rango de direcciones IP privadas desde el exterior (pruebas 1.1.3, 1.1.4.3) 3- Se identificaron por procesos automatizados de rastreo las direcciones IP de los servidores , el sistema operativo y las versiones de cada demonio (pruebas 1.1.2.1 a 1.1.2.1.4) 4- Se encontraron servicios internos (NetBEUI) visibles desde el exterior.(pruebas 1.1.2.1 a 1.1..2.1.4) 5- Los equipos de borde respondieron a consultas SNMP desde el exterior utilizando los nombre de comunidad por omisión. (Prueba 1.1.5) 6- Se identificaron las direcciones públicas disponibles mediante solicitudes ICMP. ((Prueba 1.1.3) 7- Se obtuvieron vía DNS transferencias de zonas conteniendo direcciones privadas. (Prueba 1.1.4.3) 8- Se logró armar un mapa de la red desde el exterior. (Prueba 1.2) 9-Se encontraron servicios con múltiples vulnerabilidades y sistemas no actualizados. (Prueba 1.3) **NIVEL DE RIESGO: ALTO**
Generar condiciones de Negación de Servicios.	1-Se logró enviar mensajes ICMP a la dirección de difusión (broadcast) de la red auditada desde el exterior. Esta condición puede utilizarse para provocar ataques tipo smurf. (Prueba 2.1) 2- Los servidores de correos fueron afectados por pruebas de stress con tamaños de correos significativos (Prueba 2.2). 3- El servidor WEB (Apache sobre windows 2000) se vio afectado por inundación SYN. (Prueba 2.1) **NIVEL DE RIESGO: ALTO**
Pruebas contra firewalls	1-Aparentemente, en este momento solo se hacer pruebas de penetración, la política por omisión del firewall es Aceptar todo lo que no esté explícitamente prohibido o existe una regla extremadamente permisiva en el inicio. (Pruebas 3.1 y 3.2) 2- Se pudo identificar las interfaces y modelo de firewall haciendo solicitudes SNMP y conexiones directas al mismo. (Prueba 3.1.1) 3- Los paquetes ICMP atraviesan el firewall y llegan a los dispositivos de las zonas protegidas. (Prueba 3.2) **NIVEL DE RIESGO: ALTO**

Sección	Hallazgos
Identificar vulnerabilidades en Servidores WEB	1- Los servidores Web se encontraban desactualizados con versiones vulnerables cuyos "exploits" están disponibles en Internet. (Prueba 4.1) 2- Aparentemente los servidores explorados están configurados con las opciones por omisión. **NIVEL DE RIESGO: MEDIA.**
Identificar errores básicos de configuración en servidores SMTP	1- Se logró enviar correos desde direcciones y con destinos falsos. Lo cual implica que el servidor puede ser utilizado como "relay" (Prueba 5.1) 2- Se enviaron adjuntos normalmente no permitidos (ej. imágenes gif) (Prueba 5.2) 3- Se enviaron adjuntos de cualquier tamaño. (Prueba 5.3) **NIVEL DE RIESGO: ALTA**
Identificar errores básicos de configuración de ambientes inalámbricos	No Aplica. El sitio auditado no posee instalaciones inalámbricas.
Identificar errores de la configuración básica de servidores UNIX ó GNU/Linux	1- Se encontraron varias contraseñas débiles en las cuentas de correo. Se recuperaron algunas banderas[302] para servir de evidencia. (Prueba 7.1) 2- Se lograron establecer conexiones X al servidor con SO RedHat 9.0 (Prueba 7.2) 3- Se encontraron múltiples vulnerabilidades asociadas a la desactualización del sistema operativo y las aplicaciones que se ejecutan.(Prueba 7.4) **CONDICION DE RIESGO: ALTA**
Fisgonear información sensible de la red	No aplica, debido a las condiciones en que se diseñaron las pruebas en el módulo 1.
Identificar errores básicos de configuración en servidores Windows	1- Se consiguieron usuarios con claves muy débiles que fueron rotas con sencillez. (Prueba 9.1) 2- No existen políticas de bloqueo de cuentas. (Prueba 9.2) 3- Se logró instalar un troyano y se tomó control de máquinas clientes.(Prueba 9.3) 4- Se encontraron unidades compartidas sin seguridad adecuada. (Prueba 9.3)

[302] Por regla general al ejecutar este tipo de pruebas se dejan archivos como evidencia de la posibilidad de escribir en el sitio penetrado (poder escribir implica también poder cambiar información y posiblemente incluso borrarla). Este tipo de evidencia dejada por el auditor se denomina bandera.

Sección	Hallazgos
	5- Se logró obtener la clave de administrador del dominio. Esta es la condición más crítica obtenida. (prueba 9.3) **CONDICION DE RIESGO: ALTA**

Tabla 3: Resumen de los resultados fundamentales de la ejecución del Módulo Pruebas de Penetración

2.1 Algunas evidencias recabadas durante la ejecución de las pruebas de penetración

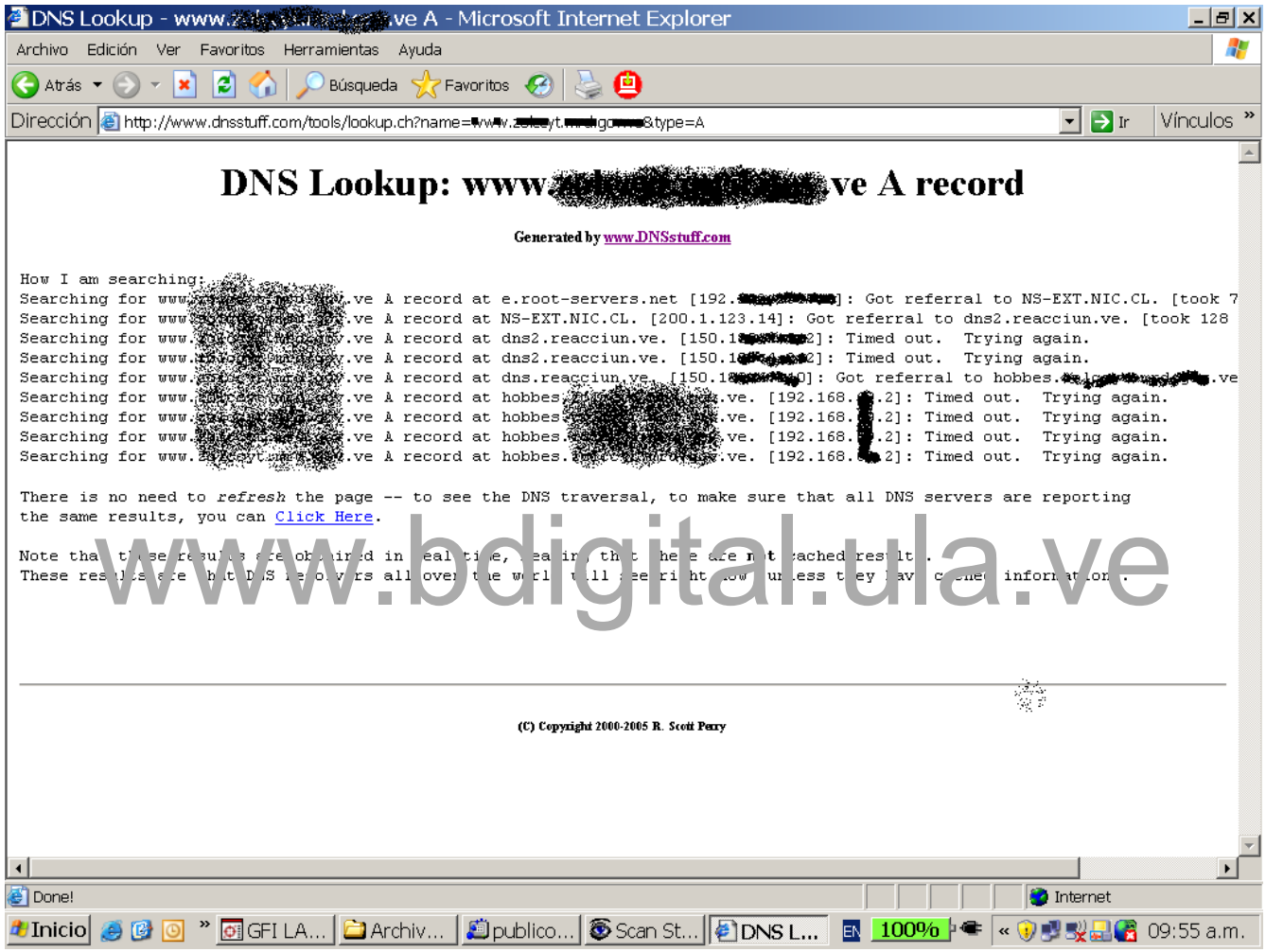


Ilustración 7: Evidencias recabadas durante la ejecución de las pruebas de penetración. Puede notarse que se difunden por DNS direcciones privadas

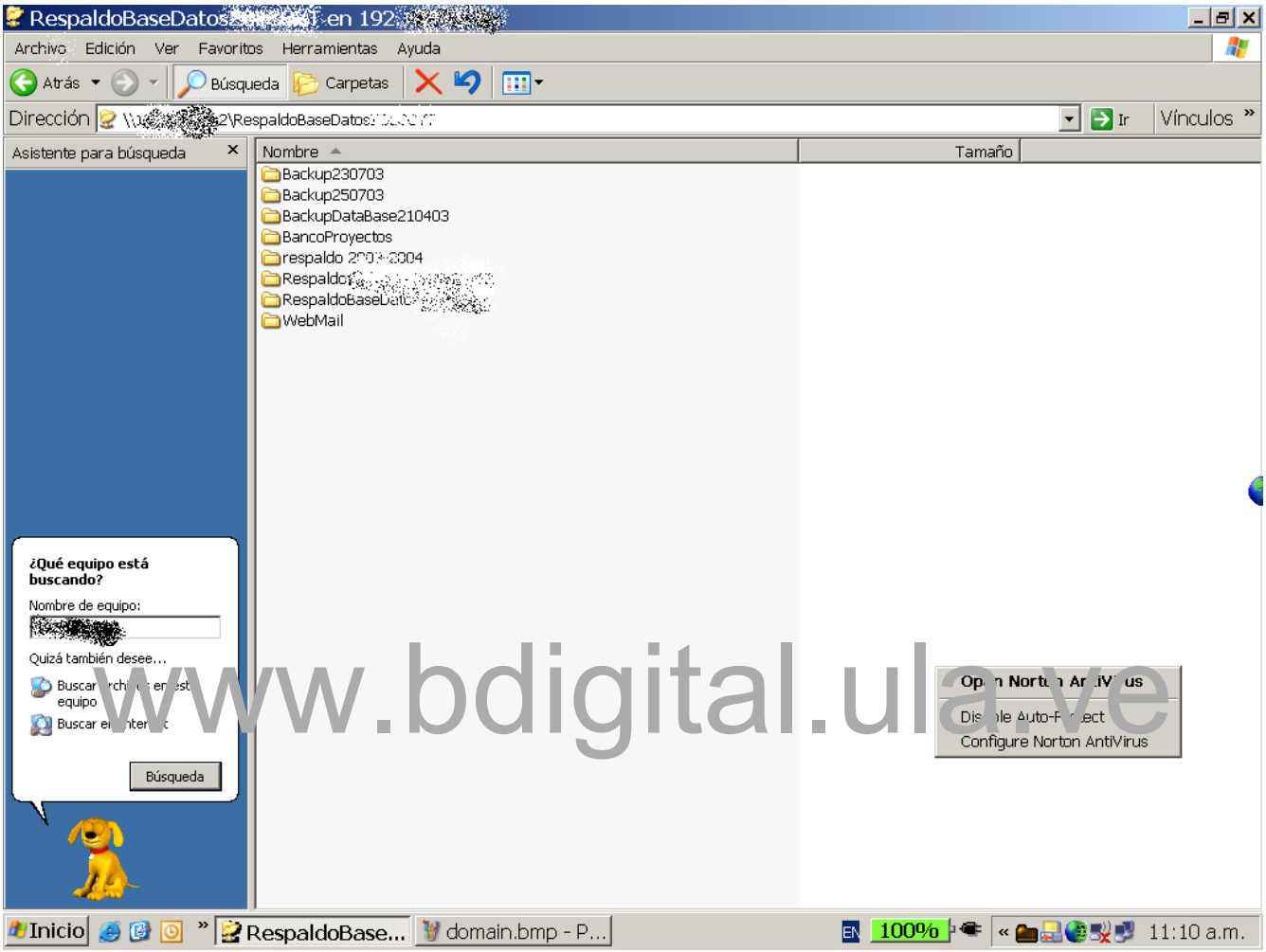


Ilustración 8: Evidencia recabada durante las pruebas de penetración. Carpetas sin los permisos correctos

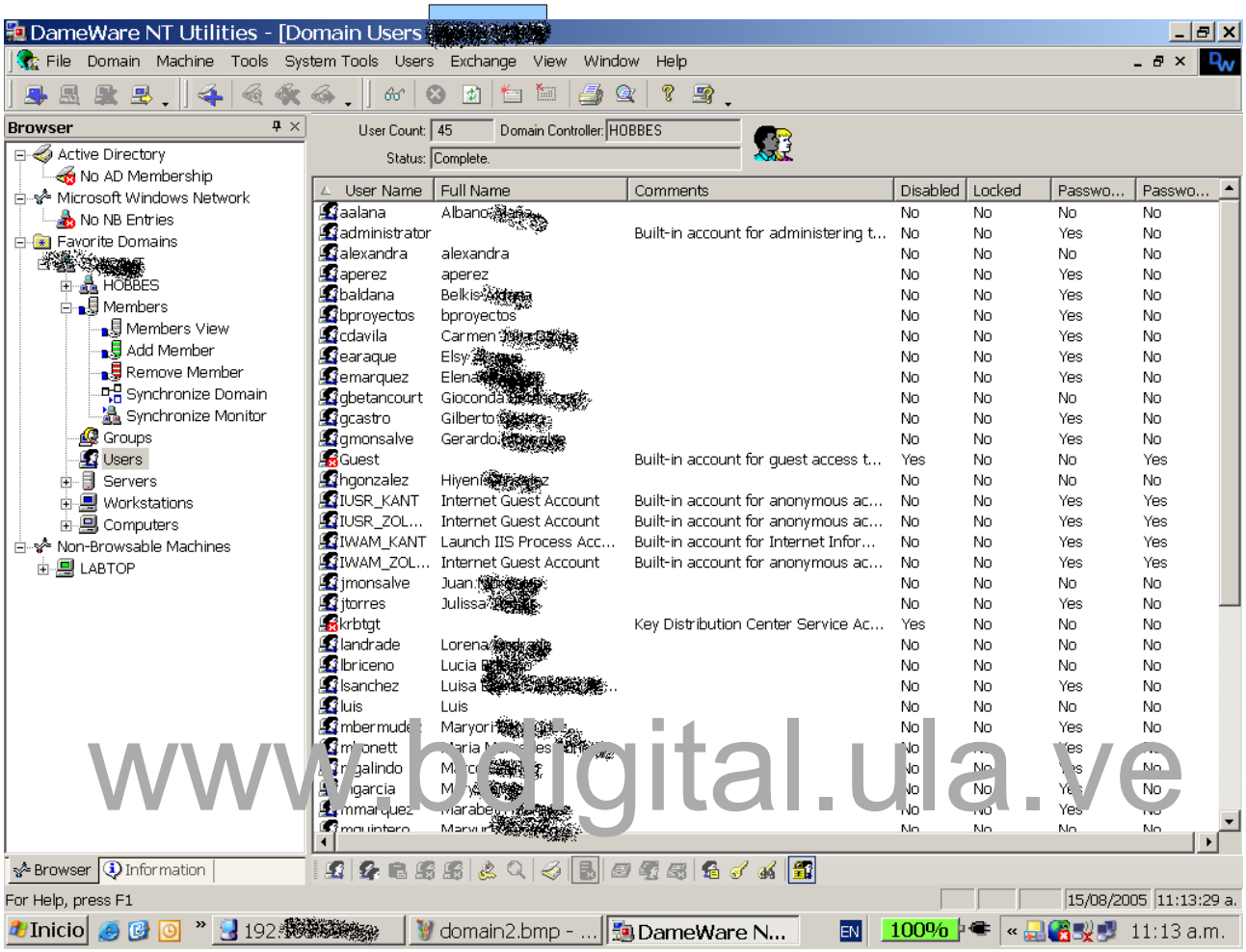
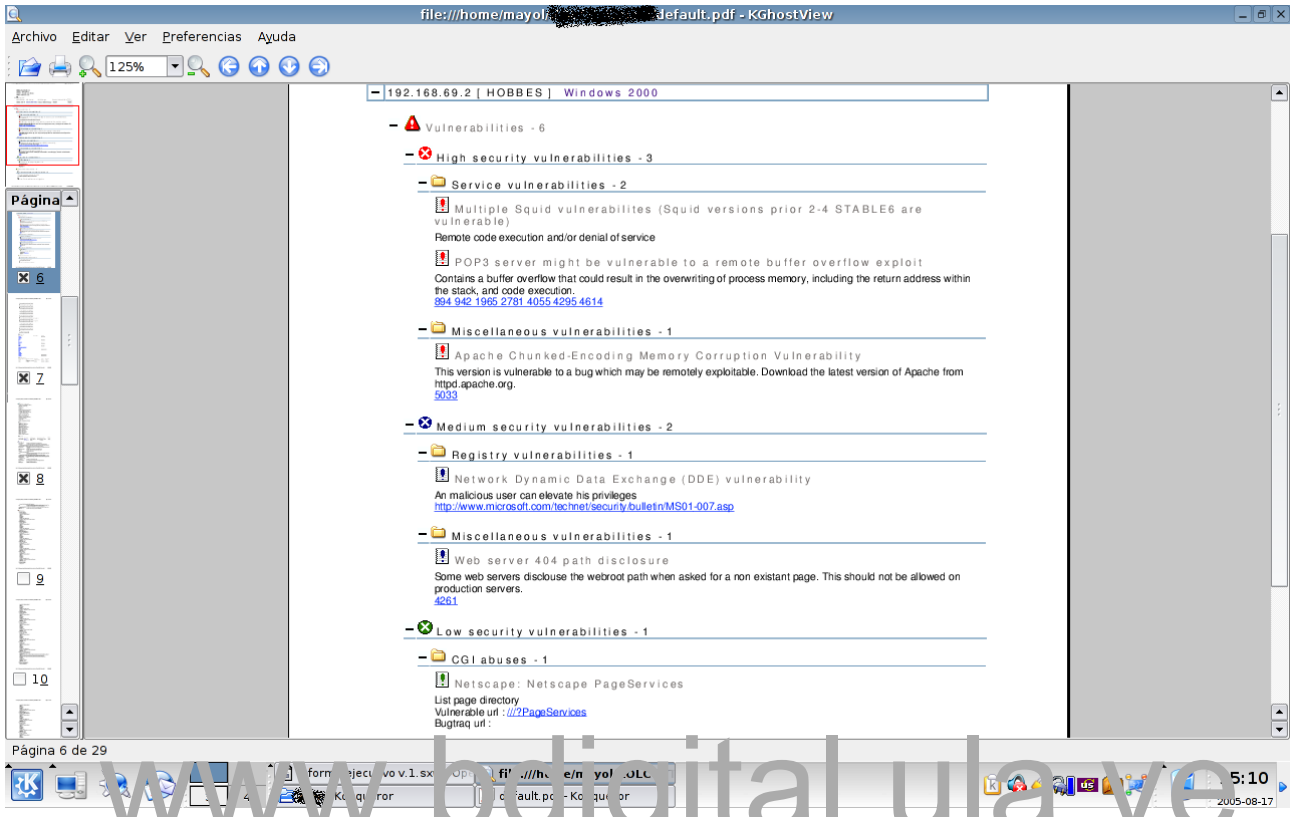


Ilustración 9: Evidencias obtenidas durante las pruebas de penetración. Una vez obtenida la clave del administrador del dominio se instaló un troyano. Utilizando el mismo se tomó control de los servidores basados en MS Windows. La figura muestra la enumeración de los usuarios. Se evidencia también la existencia de usuarios sin contraseña. Esta labor fue realizada de forma remota. Se ha enmascarado la información confidencial.

Ilustración 10: Extracto del reporte de salida de una de las herramientas de búsqueda de vulnerabilidades utilizada. Se evidencian gran cantidad vulnerabilidades detectadas. Se ha enmascarado la información confidencial.



3. Resultados de la ejecución del módulo: Revisiones.

A continuación se ofrece un resumen de los hallazgos más significativos, los cuales fueron todos encontrados utilizando el modelo que se propone en este trabajo. Como en el caso de las Pruebas de Penetración, parte de la información ha sido omitida o cambiada tomando en cuenta la necesidad de mantener su confidencialidad. Una vez terminado el ejercicio de auditoría, el sito bajo estudio fue sometido a un intenso trabajo de correcciones de las condiciones encontradas. Este trabajo incluyó la reinstalación de la mayoría de los servidores, la instalación de un nuevo dispositivo firewall, la instalación de varios sistemas de detección de intrusos y el replanteamiento de la forma en que información confidencial se transfería desde y hacia la organización.

Sección	Hallazgos mas significativos.
Seguridad Física	1. Los equipos no encuentran en ambientes adecuados en cuanto a: control temperatura y humedad, limpieza, aislamiento de cargas electrostáticas, protección contra descargas eléctricas, protección contra sismos. (Regla 1.2) 2. No existen medidas para Restringir y controlar el acceso a los dispositivos de cómputo central y de comunicaciones, cualquiera sea la plataforma de procesamiento. (Prueba 1.3) 3. No existen equipos que permitan respuesta automática ante condiciones de riesgos como intrusiones físicas, incendios, temblores, aumentos buscos de la temperatura. (Regla 1.5) 4. No existen mecanismos para proteger físicamente los respaldos de información. (Prueba 1.7) 5. No existen planes de contingencia para el mantenimiento operativo ante la materialización de situaciones de riesgo físico como las mencionadas en los acápites anteriores. (Regla 1.9) 6. Verificar que existen planes de evacuación ante emergencias del personal y resguardo de los equipos principales ante la ocurrencia de imprevistos que lo ameriten. (Prueba 1.13) 7. El personal no conoce ni ha sido entrenado para utilizar los planes de contingencia mencionados en el no. 5 **8.** **NIVEL DE RIESGO: ALTO**
Revisión de Servidores basados en Unix	1. Se encontraron problemas la permisología de programas de configuración (Reglas 1.3 y 1.4) 2. No existen listas de acceso para programas de administración principales y son correctas (Regla 1.7) 3. No se utiliza el comando *umask* para normalizar la permisología de los archivos. (Prueba 1.8) 4. Se encontraron varios procesos corriendo que no son utilizados (NFS, fetchmail). (Regla 2.1) 5. Todos los servicios y el propio sistema operativo no han sido actualizados desde su instalación. (Prueba 2.5.2) 6. No se utilizan wrappers para filtrar el acceso a las aplicaciones. (Regla 2.5.3) 7. No existen políticas de conformación de contraseñas. (Prueba 3.1) 8. No se utilizan historiales del uso de contraseñas. (Regla 3.2)

Sección	Hallazgos mas significativos.
	9. No se utilizan tiempos de vida de las contraseñas. (Prueba 3.3) 10. Existen varios usuarios con contraseñas débiles (Prueba 3.4) 11. No hay programas de control de la calidad de las contraseñas. (Prueba 3.7) 12. La cuenta root se utiliza para trabajos cotidianos. (Prueba 4.1) 13. Se encontraron en las bitácoras intentos fructíferos de intrusión. (Prueba 4.8) 14. No hay políticas de respaldos regulares (Prueba 5.1) 15. No se verifican los respaldos una vez realizados. (Prueba 5.4) 16. No existen sistemas de detección de intrusos (Prueba 6.1 a 6.4) 17. Los sistemas de bitácoras están configurados por omisión y no son regularmente fiscalizados. (Prueba 7.1 a 7.7) 18. No existen filtros de paquetes (iptables) ni a nivel de aplicaciones que controlen el acceso a las mismas. (Prueba 8.1 y 8.2) **NIVEL DE RIESGO: ALTO**
Revisión de Servidores basados en Windows	1. La cuenta de administrador se utiliza para labores cotidianas en el servidor. (Prueba 1.1) 2. El sistema control de usuarios y contraseñas está configurado por omisión. No hay historial de contraseñas, ni políticas de conformación o duración de las mismas. (Pruebas 1.2 a 1.11) 3. Cualquier usuario puede iniciar sesión en los servidores. (Prueba 3.1) 4. Existen varios servicios ejecutándose no necesarios para las funciones de los servidores. (Prueba 4.1) 5. El sistema no está actualizado (Prueba 4.2) 6. No existe servicio de auditoría interna ni servicios de terceros activados para esa función (Pruebas 6.1 a 6.3)

Sección	Hallazgos mas significativos.
	NIVEL DE RIESGO: ALTO
Revisión de Servidores Sendmail	1. La opción FEATURE(`promiscuous_relay') está habilitada permitiendo relay, el cual había sido probado durante las pruebas de penetración. (Prueba 3.2) 2. La opción EATURE(`accept_unresolvable_domains') se encuentra habilitada. (Prueba 3.5) 3. La opción FEATURE ('accept_unqualified_senders') se encuentra habilitada. (Prueba 3.7) 4. La opción FEATURE(`blacklist_recipients') no se encuentra habilitada. (Prueba 3.8) 5. La opción FEATURE(`dnsbl') no se encuentra habilitada. (Prueba 3.9) 6. No se autentifican a los usuarios cuando envían correos (Pruebas 4.1 a 4.3) 7. La opción MaxMessageSize no está establecida. (Prueba 5.2) 8. La opción MaxRecipientsMessage no está establecida. (Prueba 5.5) 9. La opción BadRcptThrottle no está establecida (Prueba 5.6) **NIVEL DE RIESGO: ALTO**
Revisión de Servidores Apache	1. No se encontraron servicios de filtrado de acceso (Apache Mod. Security) (Prueba 3.7.6) **NIVEL DE RIESGO: BAJO**
Revisión de la Infraestructura Inalámbrica	1. No Aplica. El sitio auditado no posee conexiones inalámbricas.
Revisión de los Sistemas de Detección de Intrusos	1. El sistema de firewalls posee un sistema de detección de intrusos basados en red (NIDS), sin embargo este no está habilitado. (Pruebas 1.1 a 1.9) 2. No existen otros sistemas de detección de intrusos (Pruebas 2.1 a 2.4). **NIVEL DE RIESGO: ALTO**
Revisión de dispositivos firewalls	1. El sitio auditado posee un firewall pero la política por omisión es permitir todo. (Todas las reglas fallan a partir de este descubrimiento) **NIVEL DE RIESGO: ALTO**

Sección	Hallazgos mas significativos.
Revisión de las Políticas de Seguridad	1. El sitio auditado no posee políticas de seguridad ni establecidas formalmente ni de facto. (Todas las reglas fallan a partir de este descubrimiento) **NIVEL DE RIESGO: ALTO**
EVALUACION GENERAL	**NIVEL DEL RIESGO: ALTO**

Tabla 4: Resumen de los resultados de la ejecución del Módulo Revisiones

Conclusiones y Recomendaciones

Hemos cumplido con los objetivos planteados al inicio del trabajo. Se ha obtenido un modelo extenso, que cubre las áreas más importantes para el desarrollo seguro de la Red de Datos de la Universidad de los Andes y establece los procedimientos y los mecanismos genéricos para auditarla.

Para escoger los tópicos que conformarían el modelo fue necesario definir con detalle aquellos servicios que serían auditados, el estado del arte de los mismos, sus condiciones de explotación y otros aspectos importantes, a fin de hacer que el modelo cubriese los aspectos más significativos para la seguridad informática de RedULA.

La arquitectura de TI y de seguridad de la dependencia que se utilizó para realizar la prueba del modelo fueron modificadas para atender las recomendaciones emanadas de la utilización que se propone en este trabajo. La utilización del modelo no sólo permitió detectar condiciones de riesgo en la plataforma ya existente, sino también detectar insuficiencias importantes en el dimensionamiento del equipamiento y carencias en temas vitales como las Políticas de Seguridad Informática.

Además de la dependencia donde fue probado el modelo reportada en capítulo 4 , la red del Rectorado de la Universidad de Los Andes fue auditada recientemente utilizando el modelo propuesto en este trabajo. Como resultado se encontraron varias condiciones de riesgo significativas que fueron corregidas. Luego de haber realizado las correcciones devenidas de la utilización del modelo se obtuvo (demostrados con las estadísticas de la arquitectura de monitoreo de la red) mejoras en las condiciones de seguridad.

Al utilizar un modelo que ofrece procedimientos y salidas normalizados los auditores pueden volver a auditar, una vez realizadas las correcciones, y verificar con mayor facilidad que las condiciones de riesgo detectadas han sido corregidas.

El modelo ha sido desarrollado con un enfoque intermedio entre una visión de alto nivel, muy separada de la arquitectura que soporta los servicios y una posición de muy bajo nivel que haga el modelo muy dependiente de la arquitectura. La razón de hacerlo de esta forma es obtener una herramienta útil para el encargado de auditoría pero que a su vez pueda trascender cambios simples de la arquitectura.

El modelo puede ser utilizado no sólo para auditar, puede ser visto también como una guía de mandatos básicos para asegurar un sitio. En este momento también está siendo utilizado de esa forma por el equipo de Seguridad Informática de RedULA.

Al crear un modelo que incluye una serie de reglas que pueden ser utilizadas como criterios de buenas prácticas de seguridad el modelo igualmente puede ser utilizado para la instrucción del personal técnico en los elementos básicos de seguridad informática.

Por todos los elementos antes expuestos que se han cumplido con los objetivos planteados y hemos creado una herramienta útil y versátil para la auditoría y otras funciones necesarias para la seguridad informática de la Red de Datos de La Universidad de Los Andes.

Anexos

Anexo UNIX-1 Programas SUID (Referencia para Debían Linux)

PROGRAMAS QUE DEBEN TENER PERMISOS SUID
/etc/cupos
/etc/cups/ppd
/etc/ppp/peers
/etc/chatscripts
/var/cache/man
/var/cache/man/fsstnd
/var/cache/man/cat1
/var/cache/man/cat2
/var/cache/man/cat3
/var/cache/man/cat4
/var/cache/man/cat5
/var/cache/man/cat6
/var/cache/man/cat7
/var/cache/man/cat8
/var/cache/man/cat9
/var/cache/man/oldlocal
/var/cache/man/local
/var/cache/man/X11R6
/var/cache/man/X11R6/cat1
/var/cache/man/X11R6/cat4
/var/cache/man/X11R6/cat5
/var/cache/man/X11R6/cat7
/var/cache/man/opt
/var/local
/var/log/news
/var/spool/postfix/public
/var/mail
/usr/share/cups/model
/usr/bin/wall
/usr/bin/newgrp
/usr/bin/chage
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/expiry
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/at
/usr/bin/bsd-write
/usr/bin/crontab
/usr/bin/dotlockfile
/usr/bin/mutt_dotlock
/usr/bin/mtr
/usr/bin/ssh-agent

/usr/bin/sudo
/usr/bin/sudoedit
/usr/bin/cardinfo
/usr/bin/screen
/usr/bin/procmail
/usr/bin/lockfile
/usr/bin/fileshareset
/usr/bin/kgrantpty
/usr/bin/kpac_dhcp_helper
/usr/bin/lppasswd
/usr/bin/kdesud
/usr/bin/kppp
/usr/bin/klaptop_acpi_helper
/usr/bin/pmount
/usr/bin/pumount
/usr/bin/slocate
/usr/lib/pt_chown
/usr/lib/ssh-keysign
/usr/lib/hal/hal-dmiwrapper
/usr/lib/libfakeroot-tcp.so.0.0.1
/usr/lib/libfakeroot-sysv.so.0.0.1
/usr/sbin/arping
/usr/sbin/traceroute6
/usr/sbin/postdrop
/usr/sbin/postqueue
/usr/sbin/popd
/usr/src
/usr/local/share/fonts
/usr/local/share/sgml
/usr/local/share/sgml/stylesheet
/usr/local/share/sgml/misc
/usr/local/share/sgml/entities
/usr/local/share/sgml/dtd
/usr/local/share/sgml/declaration
/usr/local/share/xml
/usr/local/share/xml/schema
/usr/local/share/xml/misc
/usr/local/share/xml/entities
/usr/local/share/xml/declaration
/usr/local/share/texmf
/usr/local/lib/python2.4
/usr/local/lib/python2.4/site-packages
/usr/local/lib/site_ruby/1.8/i386-linux
/usr/local/lib/python2.3
/usr/local/lib/python2.3/site-packages
/usr/X11R6/bin/X
/usr/X11R6/bin/xterm
/bin/su
/bin/mount
/bin/umount
/bin/ping
/bin/ping6

/sbin/unix_chkpwd
/sbin/cardctl

Anexo WIN-1 Política de Seguridad de Contraseñas para Windows 2000, 2003 y XP

A continuación se muestran las políticas mínimas de contraseñas para equipos basados en Windows.

SINTAXIS

Directiva
Configuración predeterminada
Configuración mínima recomendada

Forzar el historial de contraseñas
1 contraseña recordada
24 contraseñas recordadas
Vigencia máxima de la contraseña
42 días
42 días
Vigencia mínima de la contraseña
0 días
2 días
Longitud mínima de la contraseña
0 caracteres
8 caracteres
Las contraseñas deben cumplir los requisitos de complejidad
Deshabilitado
Habilitado
Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio
Deshabilitado
Deshabilitado

Anexo Win-2 Permisólogía Básica para sistemas basados en MSWindows

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
%programfiles%	Full Control	Full Control	Full Control (subfolders and files only)	Read & Execute, List Folder Contents, Read	Modify
%system drive%\ IO.SYS	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)
%systemdrive%	Full Control	Full Control	Full Control (subfolders and files only)	Read & Execute, List Folder Contents, Read (this folder, subfolders and files) Create Files (subfolders only) Create Folders (this folder and subfolders only)	Modify (subfolders and files only)
%systemdrive%\ autoexec.bat	Full Control	Full Control			Read & Execute (this folder only)
%systemdrive%\ boot.ini	Full Control	Full Control			Read & Execute (this folder only)

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
%systemdrive%\ config.sys	Full Control	Full Control			Read & Execute (this folder only)
%systemdrive%\ Documents and Settings	Full Control	Full Control	Full Control (subfolders and files only)	Traverse Folder/Execute File, List Folder Contents (this folder only)	Traverse Folder/Execute File, List Folder Contents (this folder only)
%systemdrive%\ Documents and Settings\Administrator	Full Control	Full Control			
%systemdrive%\ Documents and Settings\All Users	Full Control	Full Control		Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemdrive%\ Documents and Settings\Default User	Full Control	Full Control		Read and Execute, List Folder Contents, Read	Read and Execute, List Folder Contents, Read
%systemdrive%\ MSDOS.SYS	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)
%systemdrive%\ ntbootdd.sys	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)
%systemdrive%\ ntdetect.com	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
%systemdrive%\ ntldr	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)
%systemdrive%\ Temp	Full Control	Full Control	Full Control (subfolders and files only)	Traverse Folder/Execute File, Create Files/Write Data, Create Folders/Append Data (this folder and subfolders only)	Traverse Folder/Execute File, Create Files/Write Data, Create Folders/Append Data (this folder and subfolders only)
%systemdrive%\ addins	Full Control	Full Control	Full Control (subfolders and files only)	Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read (this folder, subfolders, and files)
					Modify (this folder and subfolders only)
%systemroot%	Full Control	Full Control	Full Control (subfolders and files only)	Read & Execute, List Folder Contents, Read (this folder, subfolders, and files)	Modify (subfolders and files only)

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
				Create Files (subfolders only) Create Folders (this folder and subfolders only)	
%systemroot%\ $NtServicePackUninstall$	Full Control	Full Control			
%systemroot%\ Application Compatibility Scripts	Full Control	Full Control			Read & Execute, List Folder Contents, Read
%systemroot%\ AppPatch	Full Control	Full Control			Read & Execute, List Folder Contents, Read
%systemroot%\ Cluster	Full Control	Full Control			
%systemroot%\ Config	Full Control	Full Control			Read & Execute, List Folder Contents, Read
%systemroot%\ Connection Wizard	Full Control	Full Control			Read & Execute, List Folder Contents, Read
%systemroot%\ Connection Wizard	Full Control	Full Control			Read & Execute, List Folder Contents, Read

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
%systemroot%\ CSC	Full Control	Full Control			
%systemroot%\ debug	Full Control	Full Control	Full Control (subfolders and files only)	Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemroot%\ Debug\UserMode	Full Control	Full Control		Traverse Folder/Execute File, List Folder/Read Data, Create Files/Write Data (this folder only)	Traverse Folder/Execute File, List Folder/Read Data, Create Files/Write Data (this folder only)
				Create Files/Write Data, Create Folders/Append Data (files only)	Create Files/Write Data, Create Folders/Append Data (files only)
%systemroot%\ Driver Cache	Full Control	Full Control		Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemroot%\ Help	Full Control	Full Control			

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
%systemroot%\ inf	Full Control	Full Control		Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemroot%\ installer	Full Control	Full Control			Read & Execute, List Folder Contents, Read
%systemroot%\ java	Full Control	Full Control	Full Control	Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read (this folder, subfolders, and files) Modify (subfolders and files only)
%systemroot%\ media	Full Control	Full Control		Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemroot%\ msagent	Full Control	Full Control		Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemroot%\ Registration	Full Control	Full Control		Read	Read
%systemroot%\ repair	Full Control	Full Control		List contents	Modify

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
				(this folder only)	
%systemroot%\ security	Full Control	Full Control		Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemroot%\ ServicePackFiles	Full Control	Full Control			
%systemroot%\ system32\	Full Control	Full Control	Full Control (subfolders and files only)	Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemroot%\ system32\ appmgmt	Full Control	Full Control		Read & Execute, List Folder Contents, Read	
%systemroot%\ system32\ Netmon	Full Control	Full Control			
%systemroot%\ system32\GroupPolicy	Full Control	Full Control		Read & Execute, List Folder Contents, Read	Read & Execute, List Folder Contents, Read
%systemroot%\ system32\ias	Full Control	Full Control	Full Control (subfolders and files only)		

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
%systemroot%\ system32\config	Full Control	Full Control	Full Control (subfolders and files only)	Read & Execute (this folder and subfolders only)	Read & Execute (this folder and subfolders only)
%systemroot%\ system32\ NTMSData	Full Control	Full Control			
%systemroot%\ system32\spool\printers	Full Control	Full Control	Full Control (subfolders and files only)	Traverse Folder/Execute File, Read Attributes, Read Extended Attributes, Create Folders/Append Data (this folder and subfolders only)	Traverse Folder/Execute File, Read Attributes, Read Extended Attributes, Create Folders/Append Data (this folder and subfolders only)
%systemroot%\ Temp	Full Control	Full Control	Full Control (subfolders and files only)	Traverse Folder/Execute File, Create Files/Write Data, Create Folders/Append Data (this folder and subfolders only)	Traverse Folder/Execute File, Create Files/Write Data, Create Folders/Append Data (this folder and subfolders only)
c:\autoexec.bat	Full Control (this folder	Full Control (this folder			Read & Execute (this

Archivo/Subdirectorio	Administrador	Sistema	Creador/Propietario	Usuarios	Usuarios Avanzados
	only)	only)			folder only)
c:\boot.ini	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)
c:\config.sys	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)
c:\ntbootdd.sys	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)
c:\ntdetect.com	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder only)
c:\ntldr	Full Control (this folder only)	Full Control (this folder only)			Read & Execute (this folder)

Tabla 5: Permisología Básica para sistemas basados en MS Windows

Anexo PROGRAMA INSEGURO

Un programa es inseguro si, cumple alguna de las siguientes condiciones:

1. Tiene asignados más privilegios que los necesarios
2. SI SUID=1 ENTONCES{
   2.1 El programa hace más funciones para las que no se necesita SUID.
   2.2 El programa permite "escapes al Shell"
   2.3 El programa es un Shell script
   2.4 Invoca a procesos externos sin despojarse del SUID }
3. No permite utilizar ACL
4. No permite utilizar wrappers
5. Está escrito en un lenguaje que no cheque los límites (ej C) (ej. funciones como strcpy(), strcat(), sprintf(), gets() permiten escribir en memoria sin limites)
6. La gestión de archivos permite ataques de "race condition"
7. SI "utiliza temporales" ENTONCES {
   8.1 No los borra al terminar
   8.2 No se controla el tamaño
   8.3 No se hace selección correcta de los nombres}
8. Se permite libremente la creación de "core"
9. El umask heredado hace que los archivos creados por el programa estén sobreprivilegiados
10. Si se invoca al Shell sin fijar previamente el valor de las variables de entorno
11. No se validan los valores de entrada desde los usuarios.
12. Invoca a otros programas sobre los que no se tiene control.
13. Se depende de la ejecución de otros programas, pero no se tienen medidas para manejar condiciones anómalas de terminación o bloqueo de los mismos.
14. El programa no deja rastros (logs) de su funcionamiento

Anexo FIREWALLS-1 Direcciones IP que deben bloquearse según RFC 1918

- 255.255.255.255
- 127.0.0.0

Private (RFC 1918) addresses

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Reserved addresses

- 240.0.0.0

Illegal addresses

- 0.0.0.0

UDP echo

ICMP broadcast (RFC 2644)

Anexo FIREWALLS 2. Servicios que por omisión deben bloquearse en sentido Zona Externa a Zona Interna

SINTAXIS
Service
Port Type
Port Number

DNS Zone Transfers excepto desde servidores DNS secundarios si existen.
TCP
53
TFTP Daemon
UDP
69
Link
TCP
87
SUN RPC
TCP & UDP
111
BSD UNIX
TCP
512 – 514
LPD
TCP
515
UUCPD
TCP
540
Open Windows
TCP & UDP
2000
NFS
TCP & UDP
2049
X Windows
TCP & UDP
6000 – 6255
Small services
TCP & UDP

20 and below
FTP
TCP
21
SSH Y TELNET
22, 23
SMTP (excepto si existen mail relays externos)
TCP
25
NTP
TCP & UDP
37
Finger
TCP
79
HTTP (excepto para servidores externos externos)
TCP
80
POP
TCP
109 &110
NNTP
TCP
119
NTP
TCP
123
NetBIOS in Windows NT
TCP &UDP
135
NetBIOS in Windows NT
UDP
137 & 138
NetBIOS
TCP
139
IMAP
TCP
143
SNMP
TCP

161 &162
SNMP
UDP
161 &162
BGP
TCP
179
LDAP
TCP &UDP
389
SSL (excepto para servidores externos externos)
TCP
443
NetBIOS in Win2k
TCP &UDP
445
Syslog
UDP
514
SOCKS
TCP
1080
Cisco AUX port
TCP
2001
Cisco AUX port (stream)
TCP
4001
Lockd (Linux DoS Vulnerability)
TCP &UDP
4045
Cisco AUX port (binary)
TCP
6001
Common high order HTTP ports
TCP
8000, 8080, 8889

Anexo PONDERACIÓN. Ponderación referencial de las pruebas utilizadas en el modelo.

La tabla número 5muestra la cantidad de pruebas en cada sección de acuerdo a su nivel de riesgo mientras que las tablas de la 6 a la 12 muestran la clasificación referencial de riesgo asignada a cada prueba. Como se mencionó en el Capítulo 2 cada regla o incluso prueba, tiene asociado un valor ponderado de riesgo a fin de que tanto auditado como auditor puedan establecer un orden de prioridad en las correcciones que deberán realizar una vez concluido el proceso de auditoría.

La clasificación de cada regla según su nivel de riesgo ha sido realizada de acuerdo a los criterios que fueron establecidos en el acápite 2.2, Ponderación de los resultados, del capitulo 2. Nuevamente es importante definir el carácter referencial de las ponderaciones propuestas, toda vez que debe ser el auditor el que en última instancia y tomando en cuenta múltiples factores particulares del sitio auditado y del tipo de prueba que se ejecuta, defina el nivel de riesgo real que debe ser considerado.

Como fue mencionado en el Capítulo 2 la ponderación fue realizada utilizando varios criterios entre los que se incluyen elementos como el impacto real de la materialización de vulnerabilidades, la facilidad de la realización.

Sección	Nivel de Riesgo		
	Bajo	Medio	Alto
Pruebas de Penetración	3	18	61
Seguridad Física	0	5	4
Revisión de Servidores Unix	5	20	36
Revisión de Servidores y Estaciones Windows	12	25	32
Revisión de Servidores Apache	1	5	13
Revisión de Servidores Sendmail	1	11	16
Revisión de la Infraestructura Inalámbrica	1	4	10
Revisión del Sistema de Detección de Intrusos	1	5	12
Revisión de Dispositivos Firewalls	1	5	7
Revisión de las Políticas de Seguridad	0	0	55

Tabla 6: Cantidad de pruebas por nivel de impacto en el modelo propuesto

Prueba (PRUEBAS DE PENETRACIÓN)	Nivel de Riesgo
Definición de la Arquitectura sin conocimientos desde Internet	
Verificar si posible identificar "Puntos de conexión de la red con el exterior"	Alto
Verificar si se pueden descubrir la versión de los servicios visibles desde el exterior.	Alto
Verificar si se pueden descubrir información valiosa de la organización a través de los servicios visibles desde el exterior.	Alto
Buscar servicios que no debiesen ser expuestos al exterior.	Alto
Verificar si es posible identificar rango de direcciones disponibles	Alto
Verifica si es posible identificar anuncios de DNS	Alto
Verificar si se pueden definiciones de zonas	Alto
Verificar si se logra hacer transferencias de zonas satisfactorias	Alto
Verificar si se pueden hacer hacer solicitudes de direcciones que no deberían estar expuestas	Alto
Verificar si se logran identificar equipos utilizando SNMP	Alto
Recolección de los parametros de las MIB de los equipos descubiertos via SNMP	Alto
Identificación de la función de cada dispositivo	Alto
Utilizando la información de obtenida tratar de armar un mapa lo más detallado posible de la red a auditar	Alto
tilizar varias herramientas de búsqueda de vulnerabilidades y hacer un listado completo de las vulnerabilidades detectadas, eliminando aquellas que puedan ser determinadas como falsos positivos	Alto
Clasificación de las vulnerabilidades	Alto
DoS	
Realizar pruebas de stress aumentando el nivel de carga en hacia el servidor WEB para encontrar el punto de inflexión de rendimiento del servidor contra carga generada	Alto
Realizar pruebas de stress aumentando el nivel de carga en hacia el servidor SMTP para encontrar el punto de inflexión de rendimiento del servidor contra carga generada	Alto
Generar tráfico hacia los equipos de comunicaciones variando el tipo de tráfico, el tamaño de los paquetes y la velocidad de transferencia	Alto

Prueba (PRUEBAS DE PENETRACIÓN)	Nivel de Riesgo
Generar tráfico hacía en broadcast de la red	Alto
Generar tráfico SYN hacia objetivos seleccionados en la red baja prueba	Alto
Buscar evidencias sobrecarga en la red producto del tráfico generado	Alto
Buscar evidencias de detección del tráfico anormal	Alto
Identificar los servidores DNS e intentar introducir datos falsos en los mapas durante las transferencias de zona	Alto
Utilizar un programa SMBdie para generar condiciones de caída a los servidores WindowsX	Alto
En los servidores Windows. Generar tráfico mal formado desde direcciones escogidas de forma aleatoria y cambiante y verificar niveles de CPU de los sistemas atacados.	Alto
Identificar servidores WEB que realicen autentificación de entrada. Introducir contraseñas largas	Medio
Pruebas contra los firewalls	
Utilizando firewalk identificar las reglas de filtrado del firewall	Alto
Identificar reglas que afecten directamente la capacidad del firewall de dar información sobre sí mismo	Medio
Identificar reglas que limiten el acceso a servicios internos	Alto
Identificar faltas en la reglas de filtrado, especialmente determinando la existencia de reglas tolerantes	Alto
Verificar la posibilidad de pasar el firewall utilizando paquetes ICMP ECHO, ECHO REPLAY y UDP	Medio
Generar tráfico segmentado hacia dentro de la red y verificar la política de control de fragmentos del firewall	Medio
Verificar el acceso anónimo desde el exterior a servidores proxy	Medio
Pruebas contra servidores WEB	
Utilizar una herramienta especializada como Nikto para la búsqueda de vulnerabilidades en servidores WEB	Alto
Ejecutar pruebas de fuerza bruta y diccionarios para encontrar claves débiles	Alto
Obtener el archivo .htaccess (o el equivalente) utilizar una herramienta para romper las contraseñas almacenadas	Alto
Explorar la posibilidad de utilizar códigos ASP de ejemplo para explorar	Medio

Prueba (PRUEBAS DE PENETRACIÓN)	Nivel de Riesgo
código fuente de otras aplicaciones.	
Verificar si es posible descargar archivos utilizando la cadena ::DATA	Alto
Enviar secuencia GET solicitando un archivo al servidor terminada por la sentencia traslade:f.	Alto
Verificar si dentro de los archivos obtenidos se encuentran claves u otra información relevante	Alto
Verificar existen formularios sin sistemas de autentificación capcha	Medio
Explorar la posibilidad de utilizar aplicaciones tipo ISSHack para ejecutar comandos remotos a través del servidor.	Alto
Utilizar un motor de búsquedas para de sitos de administración incorrectamente indexados.	Medio
Generar procesos de inyección SQL contra el servidor	Medio
Pruebas contra los servidores SMTP	
Pasar sin helo	Medio
Enviar comando helo sin nombre de máquina	Medio
Enviar comando MAIL FROM: con un nombre aleatorio sin dominio	Alto
Enviar comando MAIL FROM: utilizando un dominio que no exista	Alto
Enviar comando RCPT TO: utilizando un usuario no local	Alto
Generar correos hacia el interior de la organización con attach normalmente no aceptados	Alto
Generar correos hacia el interior de la organización con attach de tamaño normalmente no aceptados	Medio
Generar correos hacia el interior de la organización desde direcciones reconocidas como generadores de SPAM	Medio
Pruebas contra los ambientes inalámbricos	
Utilizar herramientas de "war-driving" para identificar los puntos de acceso inalámbricos, modelos, direcciones IP, tipos de cifrado	Bajo
Clonar la dirección MAC de las estación cliente y conectarse a la red	Medio
Utilizar alguna herramienta para romper las contraseñas WEP	Alto
Utilizar herramientas para suplantar e inyectar tramas completas generando suficiente tráfico para bajar el rendimiento de la red	Medio
Pruebas contra servidores UNIX	

Prueba (PRUEBAS DE PENETRACIÓN)	Nivel de Riesgo
Ejecutar pruebas de fuerza bruta para encontrar contraseñas débiles utilizadas en los servicios disponibles	Alto
Verificar si pueden establecerse sesiones de canal trasero	Medio
Verificar si existen servicios X en servidores no protegidos	Medio
Verificar si se puede ejecutar "site exec" como usuario anónimo (FTP)	Bajo
Utilizar una herramienta de rastreo de puertos para buscar puertos altas asociados a servicios RPC	Bajo
Utilizar una herramienta de búsqueda de vulnerabilidades para encontrar errores explotables asociados a RPC.	Alto
Buscar exportaciones de subdirectorios con permisología incorrecta.	Alto
Hacer un rastreo de servidores con xhost+ habilitado	Alto
Ejecutar herramientas de búsquedas de vulnerabilidades de DNS para encontrar situaciones críticas	Alto
Ejecutar herramientas de búsquedas de vulnerabilidades de SSH para encontrar situaciones críticas	Alto
Ejecutar herramientas de búsquedas de vulnerabilidades de APACHE para encontrar situaciones críticas	Alto
Verificar si existen servidores en modo promiscuo	Medio
Captura de Información en la Red	
Seleccionar paquetes que pudiese contener información sensible de usuarios capturados mediante un programa sniffer.	Alto
Pruebas contra servidores Windows	
Utilizar una herramienta de acceso directo para buscar usuarios sin contraseñas	Alto
Utilizar herramientas especializadas para probar la política de bloqueo de cuentas por intentos no satisfactorios de acceso.	Alto
Revisión de la política de filtrado de tráfico NetBIOS	Alto
Instalar un programa sniffer especializado en contraseñas. Capturar contraseñas (hash)y someterlas a un esfuerzo de fuerza bruta	Alto
Realizar una solicitud utilizando la extensión +.htr en servidores IIS	Alto
Utilizar una herramienta de búsqueda de vulnerabilidades para encontrar situaciones erróneas en la instalación de IIS	Alto

Prueba (PRUEBAS DE PENETRACIÓN)	Nivel de Riesgo
Utilizar una herramienta que permita escalar privilegios en IIS	Alto
Utilizar una herramienta que permita generar condiciones de buffer overflow	Alto
Realizar una conexión local utilizando la cuenta comprometida y ejecutar programas para la escalada de privilegios	Alto
Utilizar una herramienta para obtener los hash de las contraseñas y utilizar una herramienta de rompimiento de claves para obtener claves del sistema	Alto
Utilizar una herramienta para acceder a los valores guardados en LSA Secret.	Alto
Utilizar una herramienta de acceso remoto para abrir una interfaz de comando en los servidores baja estudio	Alto
Instalar una herramienta en los servidores baja estudio para acceso de sesiones gráficas	Alto

Tabla 7: Ponderación referencial para la Sección Pruebas de Penetración

Prueba (REVISIÓN DE LA SEGURIDAD FÍSICA)	Nivel de Riesgo
Verificar que los equipos se encuentren en ambientes adecuados en cuanto a: control temperatura y humedad, limpieza, aislamiento de cargas electrostáticas, protección contra descargas eléctricas, protección contra sismos.	Alto
Verificar si existen medidas para Restringir y controlar el acceso a los dispositivos de cómputo central y de comunicaciones, cualquiera sea la plataforma de procesamiento.	Alto
Verificar si existen equipos que permitan respuesta automática ante condiciones de riesgos como intrusiones físicas, incendios, temblores, aumentos buscos de la temperatura.	Alto
Verificar que existan mecanismos para proteger físicamente los respaldos de información.	Medio
Verificar si existen planes de contingencia para el mantenimiento operativo ante la materialización de situaciones de riesgo físico como las mencionadas en los acápites anteriores	Medio
Verificar que existan mecanismos adicionales para la continuidad del suministro eléctrico a los centros de carga principales y que estos sistemas funcionen adecuadamente.	Alto
Verificar que existen planes de evacuación ante emergencias del personal y resguardo de los equipos principales ante la ocurrencia de imprevistos que lo ameriten	Medio
Verificar que el personal conoce y ha sido entrenado para utilizar los planes de contingencia mencionados en el no. 5	Medio
Verificar que los sistemas de suministro eléctrico se encuentren adecuadamente dimensionados y protegidos	Medio

Tabla 8: Ponderación Referencial para la sección: Revisión de la Seguridad Física

Prueba (REVISIÓN DE SERVIDORES BASADOS EN UNIX)	Nivel de Riesgo
Sistema de Archivos	
Verificar que las opciones de montaje del sistema de Archivos impida que cualquier usuario pueda montar o desmontar otros sistemas de archivos.	Alto
Buscar programas con SUID o SGID activados y comparar con lista de programas permitidos	Alto
Verificar permisólogía de programas de configuración	Alto
Verificar permisólogía de los directorios home de cada usuario	Medio
Verificar si existen listas de acceso para programas de administración principales y son correctas	Bajo
Verificar si se utiliza el comando umask y si la permisólogía asignada es correcta	Bajo
Verificar que no existan shell scripts con permisólogía SUID o SGID	Medio
Procesos Activos	
Verificar que procesos se están ejecutando sólo los procesos que se ajustan a las funciones del servidor	Alto
Verificar que el proceso de arrancada de los procesos sea correcto	Medio
Verificar que los scripts de arrancada tenga la permisólogía correcta y no puedan ser invocados por usuarios normales	Alto
Verificar que los usuarios no pueden ejecutar servicios sin control del administrador del sistema	Alto
Verificar el mecanismo de invocación	Medio
INETD:verificar que se utilicen las opciones adecuadas de seguridad	Medio
Verificar que Versión actual se la Versión mas actualizada disponible	Medio
Verificar que exista control de acceso al servicio (por media de ACL, Wrappers u otro mecanismo)	Alto
Verificar que los usuarios que se utilizan para los servicios no tengan shell válido	Medio
Verificar que los usuarios que se utilizan para los servicios no tengan home válido	Medio
Contraseñas	
Verificar si existen políticas de conformación de contraseñas.	Alto
Verificar si existen políticas de historial de contraseñas	Bajo

Prueba (REVISIÓN DE SERVIDORES BASADOS EN UNIX)	Nivel de Riesgo
Verificar si existen políticas de duración (máxima y mínima) de contraseñas	Medio
Verificar si existe shadow password	Medio
Verificar si todos los usuarios poseen contraseñas seguras	Alto
Verificar que todos quienes usan el servidor tienen su propia cuenta	Bajo
Verificar si existen programas de control de calidad de contraseñas	Medio
Verificar si existen mecanismos adicionales de control de acceso	Alto
Seguridad de Usuarios	
Verificar que varios usuarios no comparten el mismo UID	Medio
Verificar que la cuenta root no se utiliza para actividades regulares	Alto
Verificar si existen restricciones al uso del comando su	Alto
Verificar quienes pertenecen al grupo 0	Medio
Verificar que los usuarios no tienen archivos ./rhost	Alto
Verificar que el . no se encuentra en la variable $PATH	Medio
Verificar si existen restricciones al uso del comando sudo	Alto
Rastrear los archivos de bitácoras en búsqueda de intentos de escalado de privilegios	Alto
Verificar que no existan cuentas dormidas habilitadas.	Bajo
Verificar se utilice Kerberos ó MD5 Hash como mecanismos de autenticación	Medio
Verificar la información entre clientes y servidores viaje cifrada	Alto
Respaldos	
Verificar regularidad de los respaldos	Alto
Verificar política de respaldos	Alto
Verificar si se respaldan los archivos importantes del sistema	Alto
Verificar si la política de respaldo incluye la verificación de los mismos	Medio
Verificar política de almacenamiento y cuidado de respaldos	Alto
Verificar si existen varias formas de respaldo de la información completa	Medio
Detección de Intrusos	
Verificar si existen programas "IDS Target", si se ejecutan con regularidad y si sus resultados son atendidos correctamente.	Alto

Prueba (REVISIÓN DE SERVIDORES BASADOS EN UNIX)	Nivel de Riesgo
Verificar que se protejan los archivos adecuados	Alto
Verificar si existen programas IDS Host, si se ejecutan con regularidad y si sus resultados son atendidos correctamente.	Alto
Verificar que se revisen los archivos adecuados	Alto
Bitácoras	
Verificar que exista el adecuado nivel de bitácoras	Alto
Comprobar si las bitácoras están debidamente protegidas	Alto
Comprobar si todos los servicios tienen servicios de bitácoras	Alto
Verificar si las bitácoras se rotan	Alto
Verificar si las bitácoras se respaldan en otros servidores (syslog)	Medio
Verificar si se lleva registro sobre los acceso a las bitácoras	Alto
Control de Acceso	
Verificar si existen filtrado paquetes de nivel de aplicaciones	Alto
Revisar que los mecanismos establecidos filtren adecuadamente el acceso a las aplicaciones.	Alto
Revisar que los mecanismos establecidos registren adecuadamente los intentos de acceso tanto satisfactorios como fallidos	Alto
NFS	
Verificar que todas las exportaciones del sistema de archivos se realizan hacia destinos y usuarios estrictamente definidos	Medio
Verificar que el sistema obliga a los clientes a usar puertos privilegiados	Alto
Verificar que el sistema utiliza las opciones cross-check PTR y ADDR hostname lookups	Alto
NIS	
Verificar si sólo se exportan mapas a estaciones de confianza.	Alto
Verificar si se utiliza "+:" en lugar de "+::0:0:::" como marca en el archivo de passwords.	Medio
Verificar que los mapas NIS sean sólo modificables por el root	Alto

Tabla 9: Ponderación Referencial para la sección: Revisión de Servidores basados en Unix

Prueba (REVISIÓN DE SERVIDORES Y ESTACIONES BASADOS EN WINDOWS)	Nivel de Riesgo
Revisión de Cuentas de Usuarios y Contraseñas	
Verificar que no se utilizan cuantas administrativas para trabaja cotidiano	Alto
Verificar uso syskey en niveles superiores a 1.	Medio
Verificar que no se asignan permisos directamente a las cuentas	Bajo
Verificar Privilegios de usuarios buscando privilegios mínimos.	Alto
Verificar Derechos de Inicio de Sesión.	Alto
Verificar (rompiendo) longitud y calidad de las contraseñas	Alto
Verificar la existencia de usuarios sin contraseñas.	Alto
Verificar la existencia de usuarios que nunca han usado su cuenta.	Alto
Verificar la existencia de errores en la política de contraseñas.	Alto
Verificar que no se utilicen algoritmos de hash de LM.	Medio
Verificar si se utiliza Kerberos.	Bajo
Verificar si es posible utilizar Kerberos	Bajo
Verificar nivel de caché de contraseñas	Bajo
Atributos de AD	
Verificar que no se utilicen permisos a grupos locales de dominio.	Alto
Verificar quienes tiene acceso como Administradores del bosque y validar que no se tienen permisos excesivos a este nivel.	Alto
Verificar que existe protección física para los controladores de domino raíz del bosque.	Alto
Verificar se requiere aislamiento discreto de funciones y existe un sólo bosque	Medio
Verificar si los administradores de AD utilizan estaciones de trabaja particulares para las funciones de administración	Bajo
Verificar si se delegan autoridades sobre las unidades organizativas (u objetos) en lugar de designar permisos específicos para cada una.	Bajo
Verificar si se utiliza DNS integrado a A.D.	Alto
Verificar se utilice Kerberos ó MD5 Hash como mecanismos de autenticación.	Bajo
Verificar la información entre clientes y servidores viaje cifrada.	Medio

Prueba (REVISIÓN DE SERVIDORES Y ESTACIONES BASADOS EN WINDOWS)	Nivel de Riesgo
Verificación de Permisólogía	
Verificar los permisos mínimos en el sistema de Archivos	Alto
Verificar los permisos del registro del sistema.	Alto
Servicios y Actualizaciones	
Verificar que no existan servicios superfluos o no convencionales ejecutándose.	Alto
Verificar si se han instalado los parches más recientes.	Alto
Protección del stack TCP/IP	
Verificar EnableICMPRedict=0	Bajo
Verificar SynAttackProtect =2	Alto
Verificar TCPMaxConnectResponseRetransmition=2	Alto
Verificar TCPMaxHalfOpen=50	Medio
Verificar TCPMaxHalfOpenRetired=400	Medio
Verificar TCPMaxPortsExhausted=5	Medio
Verificar TCPMaxDataRetransmitions=3	Medio
Verificar EnableDeagGWDetect=0	Medio
Verificar EnablePMTUDiscovery=0	Medio
Verificar DisableIPSourceRouting=2	Medio
Verificar NoNameReleaseonDemand=1	Medio
Verificar PerfomRouterdiscovery=0	Medio
Verificar EnableDynamicBacklog=1	Medio
Verificar dynamicBlacklogGrowthDelta=10	Medio
Verificar MinimumdynamicBlacklog=20	Medio
Verificar MaximunDynamicBlacklog=20.000	Medio
Auditoría Interna	
Verifica si las políticas de auditoría están habilitadas	Medio
Verificar si se auditan sucesos de inicio de sesión	Bajo
Verificar si se audita la administración de cuentas	Alto
Verificar si se audita el acceso a los servicios de directorios	Alto

Prueba (REVISIÓN DE SERVIDORES Y ESTACIONES BASADOS EN WINDOWS)	Nivel de Riesgo
Verificar si se auditan acceso a objetos de SO	Alto
Verifica si se audita el cambio de directivas	Alto
Verificar si audita el uso de privilegios	Alto
Verificar si se audita el seguimiento de procesos	Alto
Verificar si se auditan sucesos del sistema	Alto
Seguridad en los controladores de domino	
Verificar que no se utilicen aplicaciones con contraseñas cifradas con algoritmos de doble vía.	Medio
Verificar que todos pertenezcan a una unidad organizativa común	Bajo
Verificar si existe una plantilla de seguridad de línea base y si esta se aplica a la unidad organizativa a la que pertenecen los servidores de dominio	Medio
Verificar si las plantillas de seguridad son almacenadas de forma segura.	Alto
Seguridad de Servidores DNS	
Verificar si existen zonas integradas a AD	Alto
Verificar si los servidores internos y externos son independientes.	Medio
Verificar si existen restricciones a las transferencias de zonas.	Medio
Verificar quienes y porque pertenecen al grupo DNSAdmin.	Alto
Seguridad para Terminal Services	
Verificar si la plantilla de seguridad Notssid.inf está aplicada servidores con permisos compatibles con Terminal Server 4.0.	Medio
Verificar que se ha restringido las aplicaciones disponibles para usuarios de TS.	Alto
Verificar que no está habilitado el control remoto en los servidores de TS.	Alto
Verificar que habilitado High Encryption Pack.	Medio
Seguridad para servidores DHCP	
Verificar que no exista la cuenta del servidor en el grupo DNSUpdateProxy.	Medio
Verificar que no se utilicen direcciones asignadas por DHCP para servidores.	Bajo
Verificar quienes y por qué pertenecen al grupo Administradores DHCP.	Alto
Verificar que está habilitada la auditoría de DHCP.	Alto

Prueba (REVISIÓN DE SERVIDORES Y ESTACIONES BASADOS EN WINDOWS)	Nivel de Riesgo
Seguridad de Servidores WINS	
Verificar la necesidad de mantener servidores WINS dentro del dominio.	Bajo
Verificar las replicaciones entre servidores WINS.	Alto

Tabla 10: Ponderación Referencial para la sección: Revisión de servidores basados en Windows

Pruebas (REVISION DE SERVIDORES SMTP SENDMAIL)	Nivel de Riesgo
Revisión de Versiones	
Verificar si Versión del sendmail <= 8.9.3	Alto
Verificar si versión_Demonio < versión_mas_actualizada_estable	Medio
Condiciones Generales	
Verificar con que usuario corre el demonio.	Alto
Verificar que nadie mas pertenece al grupo con que corre el demonio	Alto
Verificar que el usuario de sendmail no tiene shell válido.	Alto
Verificar permisólogía básica de los archivos de configuración y colas de sendmail.	Alto
Chequear Alias buscando entradas sospechosas .	Medio
Verificar los programas que pueden ser utilizados por el MTA en el smrsh.	Alto
Verificar permisos de archivos forward.	Alto
Verificar que cualquier usuario no pueda ver el estado de las colas de correos.	Alto
Técnicas Anti-Relay	
Verificar que no exista FEATURE ('relay_entire_domain')	Alto
Verificar que no exista FEATURE(`promiscuous_relay').	Alto
Verificar que no exista FEATURE(`relay_based_on_MX'),	Medio
Verificar que no exista FEATURE(`relay_local_from'),	Bajo
Verificar que no exista FEATURE(`accept_unresolvable_domains').	Alto
Verificar que no exista FEATURE(`accept_unqualified_senders')	Alto
Verificar si existe FEATURE(`blacklist_recipients').	Medio
Verificar si existe FEATURE(`dnsbl').	Medio
Autentificación	
Verificar si existe FEATURE(`STARTTLS').	Medio
Verificar que exista la opción SMTP_AUTH.	Alto
Verificar que sendmail obligue la autentificación de los usuarios que envían email.	Alto
Prevención de DoS	
Verificar opción MaxDaemonChildren.	Alto
Verificar opción MaxMessageSize.	Alto

Pruebas (REVISION DE SERVIDORES SMTP SENDMAIL)	Nivel de Riesgo
Verificar max_connection_rate ,max_connections ,wait_for_client ,wait_for_server.	Medio
Verificar DelayLA.	Medio
Verificar BadRcptThrottle.	Medio
Misceláneos	
Verificar si no están activadas las opcionesVRFY y EXPN.	Medio
Verificar el nivel de bitácoras que se utiliza.	Medio

Tabla 11: Ponderación Referencial para la sección: Revisión de Sendmail

Prueba (REVISION DE SERVIDORES APACHE)	Nivel de Riesgo
Condiciones Generales de Instalación	
Verificar si "$ServerRootDirectory tiene permisos 511"	Alto
Verificar si "$ServerRootDirectory es propiedad del root (root:root)".	Alto
Verificar si " el ejecutable del demonio es propiedad del root "	Alto
Verificar SI la carga de CPU no se incrementa al utilizar SSI	Medio
Verificar que el wrapper suEXEC esté configurado	Alto
Verificar que no está habilitado SSI para archivos .html o .htm	Bajo
Ambiente de Ejecución CGI	
Verificar que los usuarios no pueden ejecutar CGI en cualquier directorio.	Alto
Verificar que los CGI no ponen en riesgo la seguridad	Alto
Protección General	
Verificar que por omisión sólo se da acceso a los directorios correctos y se niega la resto.	Alto
Verificar que Versión_actual =Versión_mas_actualizada.	Medio
Verificar fortaleza de las contraseñas si se utiliza control de acceso	Medio
Verificar permisos del archivo htaccess.	Alto
Verificar que los permisos de los archivos .htaccess no sobreescriban los permisos generales del servidor.	Alto
Verificar permisos de archivos public_html	Medio
Verificar que el usuario del demonio no tenga shell válido	Alto
Verificar que el usuario del demonio no tenga home válido	Alto
Verificar que el servidor no se ejecute baja el usuario root.	Alto
Verificar que sólo se entregue la información necesaria sobre el servidor.	Medio
Verificar que existan y se mantengan bitácoras del servidor.	Alto

Tabla 12: Ponderación Referencial para la sección: Revisión de Apache

Prueba (REVISION DE DISPOSITIVOS DE DETECCION DE INTRUSOS)	Nivel de Riesgo
NDIS	
Verificar niveles de alerta y atención de las alarmas en dispositivos NDIS	Alto
Verificar niveles de Alertas	Alto
Verificar la distribución de las firmas pasadas 5 m, 12 h y 24 h .	Medio
Verificar posibilidad de llenar bitácoras del NDIS generando tráfico hostil debido a poco espacio	Alto
Verificar posibilidad de llenar bitácoras del NDIS generando tráfico hostil debido a exceso de alertas	Alto
Verificar que la información almacenada en las bitácoras sea correcta y completa para reconocer efectivamente un ataque	Alto
Verificar que las acciones provocadas por los mandatos del NDIS sean adecuada	Medio
Verificar si el NDIS no es capaz de detectar tráfico con variaciones de la taza de envíos	Medio
Verificar si NDIS no es capaz de detectar cambios en las direcciones IP de origen (spoofing)	Alto
Verificar si NDIS no es capaz de detectar ataques encapsulados en otros protocolos	Alto
Verificar si se han registrado las acciones realizadas por las pruebas anteriores	Alto
Verificar si el NDIS cubre todos los sitios en la red donde es importante que se capture tráfico	Alto
Verificar si en cada punto de captura de datos se captura la información completa.	Alto
IDS basados en host	
Verificar si todos los servidores críticos posean IDS	Alto
Verificar que todos los servicios críticos posean IDS	Medio
Verificar si la información guardada en las bitácoras de los servidores permite el funcionamiento adecuado de los IDS.	Alto
Verificar que las acciones provocadas por los mandatos del NDIS sean adecuada	Bajo
Verificar la distribución de las firmas pasadas 5 m, 12 h y 24 h	Medio

Tabla 13: Ponderación Referencial para la sección: Revisión de dispositivos de detección de intrusos

Referencias

[ECRIMW] 2004 E-Crime Watch Survey Shows Significant Increase in Electronic Crimes URL: http://www.cert.org/about/ecrime.html

[APASF] The Apache Software Foundation, Security Tips for Server Configuration, URL: http://httpd.apache.org/docs/1.3/misc/security_tips.html

[FORUG]Forum Underground, Desencriptando Passwords (.htaccess), URL: http://www.forounderground.com/index.php

[RISASE] Ristic I. (2005). Apache Security. EE.UU: O'Relly Media INC

[CEWCG] CERT Coordination Center. Windows NT Configuration Guidelines, URL: http://www.cert.org/tech_tips/win_configuration_guidelines.html

[WISCO]Windows Security. Com. IP Security for Windows 2000, URL: http://www.windowsecurity.com/whitepaper/Windows_Security/IP_Security_for_Microsoft_Windows_2000_Server.html

[SMITSW]Smith B., Seguridad en Microsoft Windows: Kit de Recursos, (2003), MacGraw-Hill Interamericana

[MICTHGO]Microsoft Tech, guía de Operaciones de Seguridad URL: http://www.microsoft.com/Latam/technet/home.asp

[CEUSC] CERT Coordination Center. Unix Security Checklist v.2.0, URL: http://www.cert.org/tech_tips/win_configuration_guidelines.html

[BAMLSS]Bauer M. Linux Server Security. (2005) EE.UU: O'Relly Media INC

[GAPUIS]Garfinkel S. Practical Unix and Internet Security 2nd Edition. (1996) O'Relly and Associates, Inc

[UWUSS]University of Washington,Unix System Security Checklist, URL: http://staff.washington.edu/dittrich/R870/security-checklist.html

[FNWSC] Fortified Networks, Inc., Wireless Security Checklist, URL: http://www.fortified.com/html/wireless_checklist.html

[CCWSC]Core Competence, Inc., Wireless Security Checklist for Small an Medium Businesses URL: http://hhi.corecom.com/wirelesschecklistforsmbs.htm

[SCANS] Stalling W. Cryptography and Network Security 2nd edition, (2001) Prentice Hall

[HMATS]Herzog P. , Metodología Abierta de Testeo de Seguridad 2.1 (2003), Institute for Security and Open Methodologies.

[BCBSI] Bradanovic T. Conceptos Básicos de Seguridad Informática, URL: http://www.bradanovic.cl/pcasual/ayuda3.html

[MSSPT] Mainstream Security INC, Security Penetration Testing, URL: http://www.mainstream.net/security_howto/security_penetration_testing.shtml

[SHENS] Stuart Mc. ,Hacking Exposed: Network Security, 4th edition, (2003), McGraw-Hill

[SILHTCP] Siles R. Hacking TCP/IP, (2003) EE.UU, GNU Free Software Foundation

[FOLVIW] Fundación OWASP, OWASP: Lista de Verificación para Intrusión en Aplicaciones Web Versión 1.1.17 (2004) URL: http://www.owasp.org

[NGSSO] Neil G. Sendmail Security, Sendmail.Org. URL: www.sendmail.com

[SHSSV] Some helpful security sendmail configuration options., URL: http://www.pantz.org

[ZWBIF] Zwicky T. Building Internet Firewalls, (2003), EE.UU: O'Relly Media Inc.

[TCHRFC] TechRepublic, Firewalls Checklist, URL: http:// www.techrepublic.og

[GPMASF]Gobierno Provincia de Menzona, Argentina. LINEAMIENTOS SOBRE SEGURIDAD FÍSICA, URL: http:// www.comip.mendoza.gov.ar/Normas/

[BORCSI] Borgelo C. ,Seguridad Informática, (2001), Argentina URL http:// www.cfbsoft.com.ar

[KLHCA] Klarp J., How to Conduct a Security Audit. (2000) ,PC Network Advisor URL: http//www.itp-journal.com

[CRISPMS] Cresson Ch., Information Security Police Made Easy, (2002) EE.UU, Pentasafe

[ISO 17799] International Standars Organization, ISO 17799