UNIVERSIDAD DE LAS CIENCIAS INFORMATICAS
UCI
FACULTAD 5 REALIDAD VIRTUAL

Test de Penetración en la Red de la Universidad de las Ciencias Informáticas.

TRABAJO DE DIPLOMA PARA OPTAR POR EL TÍTULO DE
INGENIERO EN CIENCIAS INFORMÁTICAS

Autor

Inti Jiménez Márquez

Tutores

Ing. Arian Antonio Núñez.

Ing. Idelkys Quintana Ramírez.

Ciudad de la Habana

Julio, 2008

Frase.

Amicus Plato, sed magis amica veritas (La verdad ha de primar sobre todo).

Declaración de Autoría.

Declaramos que somos los únicos autores de este trabajo, y autorizo a la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmamos la presente a los ____ días del mes de _____ del año _____.

Autor:

Inti Jiménez Márquez

_____

Tutor:

Ing. Arian Antonio Núñez.

_____

Cotutor:

Ing. Idelkys Quintana Ramírez

_____

Datos de Contacto

Nombre y Apellidos: Arian Antonio Núñez.

Edad: 25 años.

Ciudadanía: Cubano.

Institución: Universidad de las Ciencias Informáticas (UCI).

Título: Ingeniero en Ciencias de la Informáticas.

Categoría Docente: Profesor Adiestrado.

E-mail: anuneza@uci.cu

Teléfono: 837-2702.

- Asesor de tecnología y arquitectura en la Facultad 5.

Nombre y Apellidos: Idelkys Quintana Ramírez.

Edad: 28 años.

Ciudadanía: Cubana.

Institución: Universidad de las Ciencias Informáticas (UCI).

Título: Ingeniera en Telecomunicaciones y Electrónica.

Categoría Docente: Profesor Adiestrado.

E-mail: idelkys@uci.cu

Teléfono: 837-2474.

- Profesora Instructora.
- 4 años de Graduado y de experiencia.
- Varias publicaciones en eventos nacionales e internacionales: Uciencia 2005, Uciencia 2006, Uciencia 2008, Informática 2007.
- Certificación UCI en Administración de Redes con Windows Server 2003
- Ha sido Jefe de Disciplina y de Colectivo de asignatura.
- Ha tutorado tesis de Trabajos de Diploma en años anteriores.
- Fue líder del proyecto Simulador Quirúrgico de la Facultad 5
- Actualmente es asesora general del proyecto de Supervisión Energética
- Está cursando la maestría en Telemática.

Dedicatoria

A todo aquel que persigue un sueño.

Agradecimientos

A todas las personas que me han animado en la realización de este documento, para mi familia, a los que con su esfuerzo de 6 años me hicieron llegar hasta aquí, a mis tutores Idelkys e Arian, a Jandrich por haber revisado la organización del documento y la estructura, a Alexeidis por ayudarme con las referencias bibliográficas y las imágenes, a Arian gracias por ser un buen tutor y un excelente amigo, a Alexander Moreno mi oponente por contribuir a mejorar la calidad del documento, a Alejandro Lugo por la re revisión de la tesis, al profesor de seguridad informática Lázaro gracias por la consulta. A mis amistades, compañeros, a los que ya no están pero que sigo recordando como el primer día.

Resumen

Se puede entender como seguridad un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Las necesidades en esta área están experimentando un crecimiento constante, tanto por la demanda interna como por las solicitudes de terceros. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico pues no existe un sistema 100% seguro.

El ámbito del presente trabajo, se centra en el análisis de varias metodologías de test de penetración y el uso de un conjunto de herramientas especializadas en la detección de vulnerabilidades en la red de La Universidad de las Ciencias Informáticas y cómo desarrollar un sistema de pruebas de seguridad para sus distintas áreas.

Inicialmente, se hace una revisión de los diferentes test de intrusiones existentes a nivel mundial, para así determinar los pasos y herramientas que más se ajusten al entorno universitario. Además se hace una investigación minuciosa acerca del significado de los test de intrusión y su importancia para una red de computadoras. Durante el trabajo se lleva a cabo la implementación parcial de un test en el cual se demuestra cómo mediante pruebas de seguridad se logran reconocer irregularidades en los entornos que se aplican. Las herramientas utilizadas, en gran parte son multiplataforma y de distribución libre, aunque por comodidad fueron usadas versiones que corren sobre el sistema operativo Windows XP, otras, en contraposición son completamente de pago pero fácilmente pueden ser sustituidas por herramientas que brinden resultados semejantes de distribución libre.

La información recopilada durante el test muestra una visión del estado en que se encuentra el entorno informático que se ha analizado. A partir de esta información se puede reformular completa o parcialmente las políticas de seguridad del centro que lo solicite, permitiendo tener mayor seguridad frente a incidentes o mejor respuesta a estos si llegan a ocurrir.

Palabras Claves: Vulnerabilidades, test de intrusión, multiplataforma, distribución libre, sistema operativo, políticas de seguridad.

Índice

Introducción

El siglo XXI es testigo de una nueva revolución que avanza incesantemente, ya nuestra sociedad ha sido marcada por esta y nada será como antes, esta nueva era es declarada como la Era de la Información. Su característica principal es estar marcada por una progresiva revolución de las tecnologías digitales de información y comunicaciones, modificando enormemente gran parte de las estructuras de nuestra sociedad. Nuestro país no escapa de este fenómeno y en los últimos años el gobierno ha implementado una serie de proyectos que impulsaran de forma colosal todo lo que hasta ahora hayamos visto referente a las nuevas tecnologías y sus aplicaciones. La informática en Cuba camina con pasos firmes y es llamada a transformar y mejorar un sinnúmero de procesos en todos los sectores.

La información de hecho se convierte en el recurso más valioso para una organización, empresa u individuo y por tal motivo es requerido protegerla y asegurarla de forma apropiada. Al conjunto de normas, reglas y procedimientos para proteger la información se le denomina Seguridad de la información y aunque es un termino fuertemente relacionado a la seguridad informática la diferencia mas tangible entre estas dos disciplinas es que la seguridad de la información abarca un poco más que la protección de la información puramente digital, extendiéndose más allá de la información producida por medios digitales a elementos como comunicaciones, hardware y software ayudando así a proteger mucho mejor los recursos. Como insignia de todo el movimiento informático en nuestro país se levanta la Universidad de las Ciencias Informáticas, la red de computadoras más grande en expansión que existe en nuestro país y como tal se convierte en un patrón a seguir de todo el proceso que se esta llevando a acabo en nuestra sociedad convirtiendo así en un entorno que atrae novedosas aplicaciones e ideas pero a su vez también de los consabidos errores que estos procesos novedosos traen.

Hoy día hay una enorme necesidad de seguridad en las redes de computadoras. Pero esto no es casualidad, nuestra vida diaria depende de una manera impresionante de los sistemas informáticos. Además, la evolución rápida y la demanda de tecnología han traído como consecuencia que los programadores de software, en muchas ocasiones, releguen la seguridad a segunda prioridad. Y es aquí donde entonces juega un papel relevante el Hacking Ético. Esta, no es mas, que una disciplina de la seguridad de redes que se sustenta en el hecho de que para estar protegido se debe conocer

cómo operan y qué herramientas usan los hackers. Estos llamados hackers éticos o PEN-TESTER, por sus siglas en inglés desarrollan en el argot de seguridad se conoce como Prueba de Penetración. Durante este proceso se realiza una prueba manual, intensiva, controlada y de común acuerdo con el cliente, utilizando las herramientas y técnicas usadas por los hackers. De esta forma se explotan las vulnerabilidades que existan en el sistema objetivo para ganar acceso y demostrar que un sistema es vulnerable. Este tipo de prueba es favorito de las juntas directivas de las empresas porque permite realmente evaluar si una determinada compañía será víctima y que tan cercano a la realidad está el riesgo. El hacker ético se encarga de penetrar ya sea desde fuera (internet) o desde dentro de la institución el sistema de la misma.

Situación Problémica: En una red tan joven como la existente en la Universidad de las Ciencias Informáticas (UCI), se producen a diario incidentes como robo de contraseña, pérdida de datos o accesos no autorizados a documentos o recursos. A pesar de todo se cuenta con un grupo de herramientas y personal calificado para trabajar en la detección de los mismos, aunque esto se encuentra limitado solo a las áreas centrales de servicios. Lo antes planteado, sumado al gran desconocimiento de los usuarios que aun no alcanzan una cultura de seguridad informática lo suficientemente madura, dificulta enormemente el trabajo y aumenta las posibilidades de riesgos. Otro aspecto importante es la evolución acelerada de programas dañinos en la red con la posibilidad que cualquier persona pueda llevar a cabo acciones perjudiciales con un nivel básico de conocimientos en el tema. En la universidad existen varios entornos informáticos como son los proyectos productivos que cuentan con un bajo nivel de seguridad.

Problema a resolver: ¿Cómo determinar la metodología y herramientas idóneas que garanticen a detectar las vulnerabilidades que provocan fallas de seguridad en la infraestructura de red de la Universidad de las Ciencias Informáticas?

Objeto de Estudio: La seguridad Informática.

Campo de Acción: La seguridad informática en la infraestructura de red de la UCI.

Objetivo General: Proponer un test de penetración a partir de la aplicación de un grupo de herramientas que permitan la detección de vulnerabilidades e irregularidades en la red de la Universidad de las Ciencias Informáticas en función de minimizar las mismas.

Tareas Específicas:

Estudiar los principios y características que rigen la seguridad informática para conocer las bases en

que está sentado el tema actualmente.
Analizar el estado actual de los test de penetración para determinar la metodología a usar en el entorno de red de la UCI.
Realizar una propuesta de test de penetración en los entornos productivos para seleccionar las herramientas idóneas.
Implementar de forma parcial un test de penetración.
Elaborar un conjunto de medidas para la prevención de los anomalías detectadas.

Como resultado de este trabajo se pretende obtener un informe en el cual se refleje los defectos encontrados, las técnicas y herramientas utilizadas para lograr un análisis profundo. También se debe reflejar la forma de eliminar o minimizar estos defectos ya que el fin de detectarlos es en sí erradicarlos y con esto ganar en eficiencia productiva de los medios y servicios , puede que también este análisis no arroje resultados negativos en cuyo caso se puede aplicar otra herramienta diferente y si es cuestión de que no existe defectos en el sistema estudiar la configuración que tiene ese sistema y adoptarla con estándar como forma de masificar las mejoras que suponen el uso de estas herramientas. Esto lo logramos manteniendo un seguimiento del sistema y ver como influyen las modificaciones hechas.
Los Métodos científicos de investigación usados en este trabajo son el Analítico-sintético, ya que un detallado análisis nos permitió llegar a la particularidad de nuestra investigación, así como desglosar en partes importantes la investigación para obtener la esencia de cada documento estudiado, teoría planteada y otros contenidos importantes para el desarrollo de la misma. El Inductivo-deductivo, este método nos permitió darle solución al problema planteado a través de conocimientos generales sobre el tema de investigación, llegando así a conclusiones particulares Además el método de Análisis histórico lógico el cual nos permitió hacer un estudio de la evolución que presentado la seguridad informática en Cuba y el mundo durante los últimos años.

1

Capítulo 1 Fundamentación Teórica.

Introducción

En este capitulo se exponen algunos conceptos relacionados con la seguridad, la seguridad informática y como estas han evolucionado a lo largo de los años. La ciencia, la tecnología y más específicamente la informática, han contribuido notablemente al desarrollo de esta rama.

Además se tratan otros temas como son el estado a nivel mundial de los delitos informáticos y los aspectos legales relacionados con el delito informático en Cuba. También se hace breve descripción de que es un test de penetración, como está constituido, cuales son los pasos a seguir durante la ejecución del mismo y las metodologías más usadas a la hora de realizar estos. Por ultimo se habla de las normas que rigen estas pruebas y de los estándares más usados hoy en día para la ejecución de las mismas.

1.1 Evolución del término seguridad.

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). También la Biblia, Homero, Cicerón, Cesar han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno. Los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los antiguos: las pirámides egipcias, el palacio de Sargón, el templo Karnak en el valle del Nilo; el dios egipcio Anubi representado con una llave en su mano, etc.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo, para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar ya era manejado por ellos. Como todo concepto, la Seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La primera evidencia de una cultura y organización en seguridad “madura” aparece en los documentos de la Res Publica (estado) de Roma Imperial y Republicana.

El próximo paso de la Seguridad fue la especialización. Así nace la Seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la Seguridad Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma). De estas dos se pueden desprender la Seguridad Privada y Pública al aparecer el estado y depositar su confianza en unidades armadas y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero, Henry Fayol en 1919 identifica la Seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Desde el siglo XVIII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción y reducción de fallos y pérdidas han traído nueva luz a los sistemas de seguridad. La seguridad moderna se originó con al Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella

época. Finalmente, un teórico y pionero, Henry Fayol en 1919 identifica la Seguridad como una de las funciones.

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los "cerebros electrónicos", esta mentalidad se mantuvo, porque ¿quien sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados? [3]

1.2 Evolución del concepto de seguridad informática.

Hacia los años 60's, donde el surgimiento de Internet, las motivaciones de la guerra con la crisis de los misiles y el alto potencial de investigación que generan las universidades en ese momento, establecen el sustrato necesario para que se desarrollen las necesidades de protección y control, registro y seguimiento, aniquilación y supervivencia que orientan en ese momento la política internacional, donde aquel que muestre mayor capacidad de resistencia y ataque se erige como virtual beneficiado de la tensa situación mundial.

Basado en lo anterior, las fuerzas militares reciben importantes recursos económicos para fortalecer su posición de defensa y ataque, donde las operaciones en los medios tecnológicos se muestran como una ventaja y estrategia para ganar posiciones en el escenario de la tensión internacional. Es así como se inician las primeras discusiones sobre el contexto de la seguridad nacional, donde la formulación de estrategias de seguridad y dispositivos tecnológicos son elementos que fundamentarán la manera como una nación impondrá su posición frente a la crisis de una posible guerra.

Esta situación, desarrolla la industria de los sistemas operacionales, de la criptografía, de las aplicaciones automatizadas y del hardware, con lo cual se propone un nuevo desafío para la distinción de seguridad nacional. Ahora la seguridad de las naciones se basa en la información automatizada en los diferentes sistemas desarrollados e instalados, los cuales mantienen los datos y los listados impresos fundamentales para la toma de decisiones en el contexto de la situación internacional.

De ahora en adelante el concepto de seguridad informática tendrá una figuración interesante, pues se hace necesario proteger la información que se tiene, mantener un control en el acceso a la misma, por lo que se tendrá una clasificación de la información, así como establecer estrategias para darle continuidad a la disponibilidad en caso de situaciones de falla. Con esto en mente, durante los años 70's y 80's se promueven múltiples iniciativas para fortalecer el tema de seguridad informática particularmente orientado por el área técnica. Asociaciones como ACM – Association Computery Machine y IEEE – Institute of Electric and Electronic Engineers establecen líneas de acción sobre el tema, fundando grupos de investigación, conferencias internacionales y publicaciones que poco a poco formaron los primeros profesionales en seguridad informática. Así mismo, de manera paralela los interesados en la auditoría y control de los sistemas iniciaron sus foros y discusiones alrededor de una asociación que inicialmente se llamó EDPAC – Electronic Data Processing Association y que hoy se denomina ISACA – Information System Audit and Control Association. Los nuevos profesionales, denominados Auditores de Sistemas o de procesamiento de datos, se convirtieron en los aliados de los profesionales de las ciencias de la computación para comprender los pormenores de un adecuado seguimiento y registro para mantener los ya conocidos y aceptados principios de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

Con la popularización de Internet, el fuerte desarrollo de la computación y la mayor interconexión de las organizaciones, la seguridad informática enfrenta durante la década de los 90's un nuevo desafío: seguridad distribuida. Mientras en las décadas anteriores el detalle de la seguridad giraba entorno al aseguramiento de características de software generalmente para uso local o personal, los profesionales de la seguridad informática debían ahora pensar tanto en la seguridad local como en la seguridad en la interacción con un tercero. En este sentido las primeras iniciativas se fundaron alrededor de los estándares del DoD en el año 1985, denominados Rainbow Series: libro naranja, libro rojo, libro púrpura, entre otros.

Si bien estos primeros estándares permitieron allanar el camino para las investigaciones posteriores, seguían concentrados en aspectos técnicos de los productos o implementaciones computacionales.

Particularmente durante los 90's la tecnología relacionada con la seguridad informática tuvo un amplio y sostenido desarrollo. Técnicas como las de control de paquetes de comunicaciones, cortafuegos, detección de intrusos, redes virtuales privadas, criptografía asimétrica, biométricos, filtros de correo electrónico, entre otras, recibieron gran acogida por la industria, generando variedad de productos y conceptos que son utilizados por las diferentes organizaciones tanto privadas, públicas y militares.

Esta evolución intuitiva de la seguridad informática, no sería posible sin la equivalente evolución de la calidad y sofisticación de los ataques desarrollados por los intrusos. No se puede negar la importancia de las creativas maneras de confrontar y vulnerar las soluciones de seguridad planteadas durante estos años, pues sin ellas las mejoras planteadas a la fecha no tendrían la formalidad y dimensión que se plantea en los productos actuales de seguridad.

En este punto de la revisión de la historia de la seguridad informática pareciera que la cultura y visión de los usuarios con relación a la seguridad han pasado desapercibidos, sin un papel protagónico en el concepto de seguridad. Después de los 80's y entrados los 90's las organizaciones están basadas en redes de comunicaciones que requieren una especial coordinación por parte de los individuos en las organizaciones.

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos quienes les tocan decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre Seguridad. En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

Es en este proceso en donde se aprecia que no se ha añadido ningún nuevo concepto los ya conocidos en la antigüedad; los actuales sólo son perfeccionamientos de aquellos: llaves, cerraduras, cajas fuertes, puertas blindadas, trampas, vigilancia, etc. [4]

1.3 Panorámica actual.

Muchas empresas de seguridad han empezado a ofrecer servicios de test de penetración, lo cual ayuda a generar mayor confianza en este tipo de asesoría. Además se ha desarrollado alrededor de todo esto una especie de código de honor y contratos especiales que se firman entre los auditores y las compañías usuarias, para mayor protección de estas últimas. En este contrato se estipula que la empresa da permiso para realizar la intrusión, se marca el tiempo de duración del ataque, disponibilidad de fechas para hacerlos y la forma en cómo se van a entregar los resultados, que generalmente es a manera de un reporte, donde se enumeran las vulnerabilidades y fallas encontradas, así como las recomendaciones para mitigar los problemas y optimizar la seguridad.

Aparte, se incluye una cláusula de confidencialidad, donde se asienta que la organización no puede revelar el tipo de servicio que se les ofreció, esto por propia protección del auditor, puesto que alguien podría intentar la coerción para revelar lo encontrado y atacar a la empresa. De igual forma, el contrato estipula que el auditor no puede hacer públicas las vulnerabilidades encontradas en la empresa cliente, ni quedarse con una copia del reporte final generado para la empresa, si lo hiciera se haría acreedor a una demanda.

También se pone bajo la lupa a la red interna, en donde se intenta, la penetración, se prueban contraseñas, se analizan vulnerabilidades en servidores y aplicaciones, así como avenidas de acceso. El paquete incluye también revisar módems, VPN, página Web e incluso se hace ingeniería social, es decir se trabaja con el personal o con los asociados de la empresa para ver si se dejarían engañar para proporcionar contraseñas o acceso a la red. De igual forma se mide el nivel de respuesta a incidentes internos, también se busca emular si un empleado de bajos privilegios podría tener acceso a los estados financieros o a la nómina de la compañía. Se consideran además los valores de los activos, la criticidad de la vulnerabilidad y la probabilidad del ataque, su impacto, la forma de corregirlo y el esfuerzo requerido para esto.

1.4 Estado en Cuba.

En Cuba se dio el primer paso en este sentido, con la promulgación de textos legales, aunque no precisamente penales. Entre ellos aparece el Reglamento de Seguridad Informática emitido por el Ministerio del Interior, que entró en vigor desde Noviembre de 1996, el cual estipula que en todos los Órganos y Organismos de la Administración Central del Estado se deberán analizar, confeccionar y aplicar el "Plan de Seguridad Informática y de Contingencia"; y el Reglamento sobre la protección y seguridad técnica de los sistemas informáticos

El incremento en pocos años de los delitos informáticos es significativo, de menos de 50 casos identificados entre los años 1995 al 2000 en Ciudad de la Habana, vemos que del 2001 al mes de Julio del 2004 se han incrementado de 5 a 6 veces su incidencia, igualmente vemos que en el año 2006 se ha elevado varias veces la incidencia comparada con el 2005. Se peritó hasta el año 1998 un pequeño número de casos con menos de 160 evidencias. Con el aumento de la incidencia entre los años 1999 al 2002 se obtuvieron más de 1000 evidencias y 1500 huellas, este incremento notorio obligó en el año 2000 a la creación de la Sección de Informática.

A través del Decreto Ley No. 219, de fecha 25 de abril del 2001, se crea el Ministerio de Auditoria y Control (MAC) encargado de dirigir, ejecutar y controlar la aplicación de la política del Estado y del Gobierno de Cuba en materia de Auditoria Gubernamental, Fiscalización y Control Gubernamental; así como para regular, dirigir y controlar metodológicamente el Sistema Nacional de Auditoria, con el objetivo de fomentar y preservar la probidad y disciplina en la administración de los recursos del Estado, desarrollar una cultura de la responsabilidad, prevenir y detectar actos de corrupción administrativa y, en consecuencia, garantizar la adecuada utilización y protección de dichos recursos. A su vez, el Comité Ejecutivo del Consejo de Ministros en el Acuerdo No. 4045, de fecha 31 de mayo del 2001, aprueba las funciones, atribuciones especificas y la estructura del Ministerio de Auditoria y Control. [14]

1.5 Jurisdicción y competencia penal.

En la actualidad el potencial informático de nuestra nación se encuentra distribuido a lo largo de todo el país fundamentalmente en la gestión empresarial y de forma más específica en el sistema hotelero según el promedio de los casos procesados, según registros de DTI de Ciudad de la Habana hasta mediados del año pasado. Dentro de los niveles donde incide con mayor fuerza este delito se encuentran: tiendas de recuperación de divisas; cafeterías; restaurantes y cabaret; almacenes; centros de distribución o ventas donde se facturan mercancías; oficinas de la Aduana General de la República. Esto se debe al uso imprescindible de los servicios computarizados para llevar a fondo el control de las actividades que allí se realizan y para estar en concordancia con el desarrollo internacional procurando con ello una competencia mas reñida; lo que trae como consecuencia negativa una gama de delitos propios de países capitalistas o en vías de desarrollo.

Según los datos registrados y en obtenidos en el conocido DTI de Ciudad de la Habana para conocer la forma de proceder de los delincuentes, autores de los delitos acaecidos, que fueron objeto de procesos de investigación, fue necesaria la confesión de los acusados, realizando con cada uno de estos una de las principales acciones de instrucción: reconstrucción de los hechos; ya que se desconocía totalmente por la entidad la forma o método de ejecución de estos actos y se pudo conocer además la definición detallada para establecer la responsabilidad individual de cada uno. Aunque vale destacar que se están desarrollando el desarrollo de las técnicas criminalísticas al respecto desde el mismo momento en que se constituyó un departamento encargado explícitamente a estos fines.

Ahora bien, aceptada una clasificación de los delitos informáticos, de acuerdo a las manifestaciones que las conductas delictivas han ido desarrollando, nos queda ratificar lo que al comienzo de la presente investigación precisamos con relación a estas nuevas conductas: ¿Constituyen una nueva categoría delictiva, o simplemente son formas más actualizadas de cometer viejos delitos? Esta disyuntiva se presenta atento a que la criminalidad informática revela estructuras esencialmente similares a la de los tipos delictivos ya contemplados en nuestra legislación punitiva vigente, situación en que pudiera contemplarse esta nueva conducta dentro de las figuras convencionales que se le atemperan, ya que su relación partirá de los elementos constitutivos de la figura, mas no en el mecanismo de llevar a cabo el delito, actuando esta nueva conducta como instrumento. Ejemplos de nuestro ordenamiento penal lo son

los artículos: 334; 320; 319; 318; 310; 311.c; 289; 250 – 258; que tipifican la estafa, injuria, calumnia, difamación, corrupción de menores, violación del secreto de la correspondencia y revelación del secreto de la correspondencia, falsificación de documentos, entre otros. Pero por otro lado, debe reconocerse que existen conductas especificas, penalmente reprochables, que solo pueden concebirse en su relación con un sistema informático, como los casos de los llamados en la jerga informática Hackers, el llamado pirata informático, el acceso no autorizado a un sistema informático, etc., e incluso a los programadores de virus. [1]

1.6 Estado a nivel mundial de delitos informáticos.

En la rama dedicada a las investigaciones de seguridad se descubre, investiga e informa sobre las avanzadas amenazas. Algunos líderes mundiales en investigación de seguridad, publican sus resultados para conocimiento de todos, he aquí algunas predicciones:

Olimpíadas: nuevos ataques cibernéticos, phishing y fraude:

Los ataques basados en acontecimientos y estafas son populares, y con todo el mundo atento a los Juegos, es posible que las Olimpíadas de 2008 fomenten un súbito incremento en los ataques cibernéticos. Mientras arde la antorcha olímpica, los investigadores de predicen la posibilidad de ataques de denegación de servicio a gran escala en sitios relacionados con las Olimpíadas de Pekín como declaraciones políticas e intentos de fraude a través del correo electrónico y la Web en torno a las Olimpíadas. Asimismo, se prevé peligros para los populares sitios de noticias sobre las Olimpíadas u otros sitios de deportes —ataques diseñados para instalar códigos maliciosos en máquinas de usuarios finales y robar información confidencial personal o comercial.

Ataques Web en plataformas cruzadas:

La popularidad de las computadoras Mac y los teléfonos iPhone genera incrementos Con la popularidad de la marca y el creciente uso de iPhones y computadoras Macintosh, los investigadores predicen que los atacantes lanzarán cada vez más ataques Web de plataformas cruzadas que les permitan detectar el sistema operativo en uso y faciliten la colocación de código destinado específicamente a ese sistema

operativo en lugar de ataques basados en el navegador Web únicamente. Los sistemas operativos objetivo ahora incluyen Mac OSX, iPhone y Windows.

SPAM malicioso invade blogs, motores de búsqueda, foros y sitios Web:

Los hackers utilizarán cada vez más spam web para publicar URLs a sitios maliciosos desde foros, blogs, secciones de comentarios o respuesta de sitios de noticias y en sitios Web que se han visto comprometidos. Esta actividad no sólo promueve el tráfico a los sitios Web infectados sino que también colabora para que el sitio proveedor avance posiciones en los rankings de motores de búsquedas, de modo que se incremente el riesgo de que los usuarios visiten el sitio.

Los atacantes utilizan 'vínculos débiles' de la Web para lanzar ataques:

La Web es un enredo de enlaces y contenidos. El advenimiento de adiciones Web 2.0 como Google Adsense, mash-ups o aplicaciones Web híbridas, widgets y redes sociales junto con las cantidades masivas de anuncios Web vinculados a páginas Web ha aumentado las probabilidades de 'vínculos débiles' o sitios Web y contenidos vulnerables a riesgos de seguridad. Se prevé que los atacantes explotarán cada vez más los vínculos débiles dentro de la infraestructura Web para atacar a la mayor cantidad de usuarios de Internet. Los objetivos más vulnerables de estos ataques son los motores de búsqueda y las redes de grandes usuarios como MySpace, Facebook u otros sitios de redes sociales.

La cantidad de sitios Web comprometidos superará la cantidad de sitios maliciosos que se generen:

La Web como vector de ataque ha ido aumentando a niveles constantes durante los últimos cinco años y ahora los atacantes utilizan sitios comprometidos como plataformas de lanzamiento —incluso más que los sitios creados por ellos mismos. Los sitios comprometidos —particularmente, sitios muy visitados por usuarios finales, como el ataque del Dolphin Stadium que ocurrió unos pocos días antes del Súper Bowl XLI de 2007 en Miami— proporcionan a los atacantes el tráfico Web incorporado y minimizan la necesidad de utilizar señuelos a través del correo electrónico, la mensajería instantánea o las publicaciones Web.

Incremento en los ataques Web 2.0 dirigidos a grupos de intereses especiales:

Hackers que apuntan a grupos específicos de personas sobre la base de intereses y perfiles La Web 2.0 ha generado la proliferación de usuarios Web que visitan salas de chat, sitios de redes sociales y sitios Web de intereses especiales como sitios de viajes, automotrices y más. Estos sitios permiten a los hackers encontrar víctimas potenciales que corresponden a grupos de una determinada edad, poder adquisitivo o hábitos de compra específicos. En 2008, se prevén que los ataques con objetivos aumentarán hacia redes sociales específicas o sitios de intereses especiales que presentan mayores probabilidades de rendimiento.

Técnicas de animación 'morphing' de Java Script para evadir programas de antivirus:

Los hackers están subiendo la apuesta inicial con técnicas de evasión que utilizan Java Script polimórfico (Polyscript): esto significa que se facilita una página web de código único para cada visita por parte de un usuario a un sitio web malicioso. Al cambiar el código en cada visita, a las tecnologías de detección de seguridad basadas en firmas se les dificulta la detección de páginas web como maliciosas y los hackers pueden prolongar el tiempo de ataque del sitio malicioso mientras evaden la detección.

Aumenta la sofisticación de métodos de encubrimiento de datos:

Un mayor uso de criptovirología y sofisticación en el encubrimiento de datos, incluido el uso de estenografía, datos incorporados con protocolos estándar y posiblemente dentro de archivos de medios. Los kits de herramientas que actualmente se encuentran fácilmente en la web serán utilizados para incorporar información patentada y robar datos.

Las entidades a cargo del cumplimiento de la ley a nivel global tomarán medidas enérgicas sobre grupos y personas clave del ambiente de hackers:

En 2007, los ataques basados en Internet a gran escala atrajeron la atención de los directivos a cargo del cumplimiento de la ley en todo el mundo. En el 2008 se producirá el mayor quiebre y arresto de miembros clave de grupos de hackers a través de la cooperación global de agencias a cargo de la aplicación de la ley.

Combinación y aumento de vishing y spam de voz:

La vasta población de usuarios de teléfonos celulares ha crecido para formar un mercado lucrativo que permite explotar el spamming y “vishing” a cambio de ganancias financieras .Han visto un creciente aumento en la cantidad de ataques de vishing pero no en la cantidad de spam —o llamadas automatizadas proactivas. Se prevé que aumentará y se combinará el “vishing” o la práctica del uso de ingeniería social y voz sobre IP (VoIP) para obtener información personal y financiera y spam de voz — los usuarios recibirán llamadas automatizadas de voz en líneas LAN con spam de voz para intentar obtener sus credenciales por teléfono. [22]

1.7 Pilares básicos de la seguridad.

- Confidencialidad: Debe permitirse acceso a la información solo a los usuarios autorizados.
- Integridad: Es necesario garantizar que la información no sea alterada por usuarios no autorizados.
- Disponibilidad: Se requiere garantizar que los sistemas y la información estarán disponibles cuando los usuarios autorizados la requieran.

1.7.1 Principios básicos de seguridad

- Minimizar la superficie de ataque: Cada funcionalidad añadida a la aplicación aumenta en un cierto porcentaje el riesgo de seguridad de la aplicación en conjunto.
- Establecer una configuración por defecto segura: Por ejemplo, exigentes políticas de contraseña.
- Principio del menor privilegio: Únicamente se deben conceder permisos para las tareas que se van a llevar a cabo. Por ejemplo, si un servidor solo necesita acceder a una base de datos remota, esta es la única funcionalidad que debe ser habilitada.
- Principio de la defensa en profundidad: Un único control es razonable, pero diversos controles que vigilen diferentes riesgos pueden ser mejor.
- Fallos seguros: Toda situación debe ser preparada para fallar de forma segura
- Y controlada (control de excepciones).
- No confiar en los servicios de terceros: Si la aplicación recibe información de un tercero, se debe establecer controles rigurosos sobre esta interface. Es posible que la fuente externa no disponga unas políticas de seguridad sólidas.

- Segregación de funciones: Una misma persona no debe acumular todas las funciones, mejor distribuir entre diferentes perfiles.
- Evitar la seguridad por ocultación (security by obscurity).
- Arreglar fallos de seguridad correctamente: Cuando se comparte código, es posible que fallos detectados en una funcionalidad puedan afectar a otras partes de la aplicación. Es importante testear y arreglar por completo el fallo identificado.
- Mantener la seguridad simple.

1.7.2 Reglas de seguridad informática.

- Seguidamente comentaremos brevemente en qué consiste cada una de las reglas, con el fin de ofrecer una panorámica general que plantee la complementariedad de estos conceptos y las virtudes previamente comentadas:
- El menor privilegio consiste en ofrecer el acceso requerido ara adelantar la labor solicitada exclusivamente. Es decir, otorgar los permisos estrictamente necesarios para efectuar las acciones que se requieran. Ni más ni menos de lo solicitado.
- La regla de los cambios nos dice que los cambios que se presenten deben ser coordinados, administrados y considerados en función de las implicaciones de seguridad que estos revistan. Es decir, se hace necesarios que cualquier cambio considere las implicaciones de seguridad que puede tener frente a su contexto.
- La regla de la confianza establece que debemos comprender completamente los efectos de extender nuestra confianza a un tercero y solamente confiar en lo que se requiere y acuerda de la relación. La regla del eslabón más débil nos recuerda que la seguridad de un sistema es tan fuerte como el componente o relación más débil que se identifique. Esta regla nos recuerda que nuestras decisiones deben evitar introducir eslabones débiles, documentar aquellos existentes y continuamente buscarlos.
- La regla de separación sugiere que para mantener seguro algún elemento, éste debe ser separado de peligros y riesgos de su mundo alrededor. Es decir, sólo debe tener acceso el proceso, usuarios o sistema específico, con el fin de mediar cualquier intento de acceso y tener claridad de quién solicita el mismo.

- La regla de los tres procesos nos recuerda que la seguridad informática no termina con la implementación de los productos o tecnología. Es una realidad que requiere permanentemente monitoreo y mantenimiento. Esta regla fortalece la tesis de que la seguridad requiere pensamiento y estrategia, y no solamente tecnología informática.
- La regla de la acción preventiva nos alerta que la seguridad no puede ser exitosa si no viene acompañada de una aproximación preventiva. Sin una adecuada formulación de acciones preventivas la organización tendrá menos posibilidades de mantener un esquema seguro.
- La regla de respuesta adecuada e inmediata nos dice que los pasos que una organización toma cuando ha ocurrido un incidente de seguridad son tan importantes como las acciones que tomamos para prevenir el ataque. Esta regla nos recuerda que una pobre e inadecuada respuesta a una intrusión potencialmente puede causar más daño que si un intruso lo hubiese hecho en primer lugar.
- Con estas reglas en mente y operacionales en el contexto del modelo de seguridad informática corporativa, las decisiones que se tomen responderán a un mayor nivel de conciencia e integración de la directriz general de seguridad informática, tendrán sentido para los usuarios finales en sus acciones diarias y orientarán los desarrollos e implementaciones tecnológicas prevista. [17]

1.8 Estándares y metodologías actuales.

1.8.1 OSSTMM (Open Source Security Testing Methodology Manual).

- Es el estándar más completo existente en la actualidad con una metodología para la verificación de la seguridad de los sistemas y las redes que disponen de una conexión a Internet. Esta metodología, se encuentra en constante evolución y es fruto de la colaboración de más de 150 colaboradores de todo el mundo. Gracias a este número de colaboradores, el documento incorpora los más recientes cambios y nuevos desarrollos relacionados con la seguridad informática. Antes de la OSSTMM no existía ningún documento que recogiera, de forma abierta y estandarizada, las diferentes necesidades del profesional de la seguridad durante la realización de las verificaciones de seguridad. Si bien existen otras metodologías equivalentes, ninguna hasta la fecha se había publicado con la intención de estar

disponible y mantenida por la propia comunidad profesional. Al ofrecer un marco estándar y consistente así como unos resultados claramente cuantificables. Gracias a esto, es posible garantizar los resultados, la exactitud y la validez de las pruebas realizadas.

1.8.2 ISSAF.

De OISSG este es un compendio procedimientos detallados (técnicos en muchos casos) para evaluaciones de seguridad de diversos tipos de dispositivos, procedimientos administrativos y software (desde ruteadores hasta servidores Web pasando, por sistemas operativos y procedimientos de control de cambios). [14]

1.8.3 Auditoria de Seguridad Informática ISO17799.

ISO/IEC 17799 (también ISO 27002) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la comisión International Electrotechnical Commission en el año 2000 y con el título de *Information technology - Security techniques - Code of practice for information security management*. Tras un periodo de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en la norma británica British Standard BS 7799-1 que fue publicada por primera vez en 1995. ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la Información se define en el estándar como la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran). [12]

- Auditoria de Seguridad del Centro de Cómputos.
- Auditoria de Seguridad de los Sistemas Operativos.
- Auditoria de Impacto de los Riesgos de la Seguridad Informática.
- Test de Penetración e Intrusión (Ethical Hacking).

- Auditoria de Aplicaciones.
- Auditoria de Desarrollo de Software.
- Auditoria Forense.
- Auditoria de Control Interno y Monitoreo.
- Auditoria de Adquisición e Implementación.
- Auditoria de Comunicaciones.
- Auditoria de Seguridad Global.

La evaluación de vulnerabilidades tiene una enorme cantidad de escenarios. Es imposible que una sola persona domine a detalle cada arquitectura, hardware y software susceptible de ser evaluado. Toma en cuenta también las dificultades que enfrenta un proyecto tan ambicioso como ISSAF, donde el nivel de detalle y el alcance son tales que se requiere de un esfuerzo titánico para desarrollarlo y mantenerlo. [9]

1.9 Clasificación de las pruebas.

1. **EXTERNAS:** también denominadas de “caja negra” (Black Box). Simulan un ataque sobre sistemas y seguridad por medio de la información disponible desde Internet. Se concentran en pruebas de seguridad del perímetro, análisis externo de nodos y topología; recolección de información sensitiva y su explotación mediante ingeniería social; así como en revisión de la efectividad y vulnerabilidades de aplicaciones Web, routers y firewalls; “war driving” para identificar y penetrar redes inalámbricas, y “war dialing” para localizar módems abiertos. [21]
2. **INTERNAS:** Caja blanca (White Box). Revisan las vulnerabilidades frente a un atacante interno, mediante: análisis endógeno de nodos y topología; identificación de sistemas y equipo vulnerable; búsqueda y explotación de vulnerabilidades en aplicaciones, servidores, dispositivos de red, redes inalámbricas, directorios compartidos, relaciones de confianza, arquitectura de redes y niveles de seguridad en servidores. [21]

3. **CARGA ESPECIALIZADA:** Hacen énfasis en rubros como: arquitectura de red, revisión de aplicaciones (auditoria de código), dispositivos inalámbricos, ingeniería social, acceso remoto, redes privadas virtuales y relaciones de confianza. [21]

1.9.1 ¿Qué muestran las pruebas de penetración?

1. Están concebidos, diseñados y configurados para ser fáciles de utilizar.
2. Favorecen disponibilidad y funcionalidad por encima de la seguridad.
3. Manifiestan un crecimiento acelerado de la conectividad de redes y aplicaciones.
4. Experimentan nuevas vulnerabilidades con mayor frecuencia.
5. Indican una falta de conocimiento adecuado sobre los procesos, métodos y mentalidad de los agresores informáticos.

1.10 Test de Penetración e Intrusión.

Método mediante el cual se evalúa la seguridad de los sistemas de protección perimetral de una empresa así como los diferentes sistemas que están accesibles desde Internet. [21]

Los aspectos relevantes son:

1. Búsqueda de Vulnerabilidades: se refiere generalmente a las comprobaciones automáticas de un sistema o sistemas dentro de una red.
2. Escaneo de la Seguridad: se refiere en general a las búsquedas de vulnerabilidades que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles de la red y análisis profesional individualizado.
3. Test de Intrusión: se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pre-condicionales.
4. Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

5. Auditoria de Seguridad: hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas de aplicación del sistema o sistemas dentro de una red o redes.
6. Hacking Ético: se refiere generalmente a los test de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.

Test de Seguridad y su equivalente militar, Evaluación de Postura, es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneo de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

1.11 Aspectos a tener en cuenta durante un test.

Dependiendo de si el desarrollo de la prueba es conocida por el personal de informática o no. En la primera, una prueba encubierta, sólo un selecto grupo de ejecutivos la conoce. Aquí se pueden usar técnicas de Ingeniería Social para obtener información que permita el ataque. En la segunda, el personal de informática conoce sobre el PEN-TEST. La primera, evidentemente, es más real y evita que se realicen “cambios de última hora” para tratar de adecuar la red, previo a la prueba. Para la realización de una Prueba de Penetración hay varios aspectos legales que deben ser tomados en cuenta, tanto por el PEN-TESTER como por la compañía que contrata. Estos aspectos incluyen, entre otros, el tema de la confidencialidad, de forma tal que la información recibida por el consultor no sea usada más allá de los fines de la prueba.

La organización “objetivo” o aquella que contrata debe garantizar la certeza y exactitud de la información que provee al PEN-TESTER. Es decir, esta información debe ser fidedigna, de tal forma que la prueba no arroje resultados falsos. También es importante definir el tiempo total de la prueba, que debe incluir el tiempo de ejecución de la prueba y la entrega del reporte con los resultados. Esta última es también una prueba, pero más automática, realizada con un software que asocia las vulnerabilidades encontradas con computadoras, servidores y aplicaciones en una red. Dada su naturaleza automática, son limitadas

las posibilidades de simular las capacidades de los atacantes, y además, en ocasiones se obtienen "falsos positivos" o resultados que indican una vulnerabilidad que realmente no existe.

Un buen informe de los riesgos y vulnerabilidades de una empresa, derivado de las pruebas de penetración, funge como herramienta efectiva de negociación para reafirmar o vender las estrategias de seguridad, además de sostener y legitimar todo el proyecto de protección, por lo que el mencionado documento debe estar completo, bien hecho y sin errores. Entre los puntos que debe contener este informe están: un resumen para la organización que lo solicita; un análisis de los riesgos principales; recomendaciones agrupadas por tipo de dispositivo, sistema operativo, bases de datos o servidores de dominio, y las acciones concretas a seguir. Pero también deberá incluir una clasificación de riesgos, y una evaluación que considere tres conceptos: valor de los activos, nivel de debilidades y probabilidad de ataques. El Pen Test permite priorizar riesgos y proponer acciones, con acento en las áreas alrededor de las amenazas principales. Las buenas pruebas ayudan a entender por qué los problemas pueden ser críticos, mientras dan sentido y dirección a los cambios sugeridos. El plan de acción que derive de las pruebas debe considerar el impacto desde el punto de vista de la probabilidad de ataques, vulnerabilidad y valor de los activos, así como el esfuerzo a realizar en materia de planeación, implementación y administración. En todo caso, las pruebas de penetración más eficaces permiten correlacionar el impacto de los riesgos y su probabilidad, encontrando el punto óptimo para cada empresa.

El Pen Test sirve también para motivar el cambio hacia el incremento de controles, enfocar los esfuerzos técnicos, generar conciencia y sentido de urgencia. Pero, si de verdad se quiere lograr esto es necesario organizar una demostración final de los ejercicios de irrupción. Y para cerrar el círculo conviene también organizar una reunión técnica con el fin de valorar a detalle los hallazgos, definir la forma de presentarlos a la alta dirección y trazar la estrategia a seguir. Entre las prohibiciones a fijar entre quienes ejecutarán las pruebas están; no instalar jamás puertas traseras (back doors), ni ocultar aplicaciones de acceso remoto (bots, troyanos, rootkits y demás); no borrar, alterar o inhabilitar registros y, desde luego, no apagar o modificar el comportamiento de las herramientas de detección establecidas.

Entre los puntos que debe contener el informe posterior a las pruebas de penetración están; un resumen para la alta administración; un análisis de los riesgos principales; recomendaciones agrupadas por tipo

de dispositivo, sistema operativo, bases de datos o servidores de dominio y las acciones concretas a seguir. [21]

1.12 Mapa de Seguridad.

El mapa de seguridad es una imagen de la presencia de seguridad. Esta corresponde al ambiente de un análisis de seguridad y está compuesta por seis secciones equivalentes a las de este manual. Las secciones se superponen entre si y contienen elementos de todas las otras secciones. Un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones [referirse a la figura 1.1], directa o indirectamente. [21]

Estas son:

- Seguridad de la Información.
- Seguridad de los Procesos.
- Seguridad en las tecnologías de Internet.
- Seguridad en las Comunicaciones.
- Seguridad Inalámbrica.
- Seguridad Física.

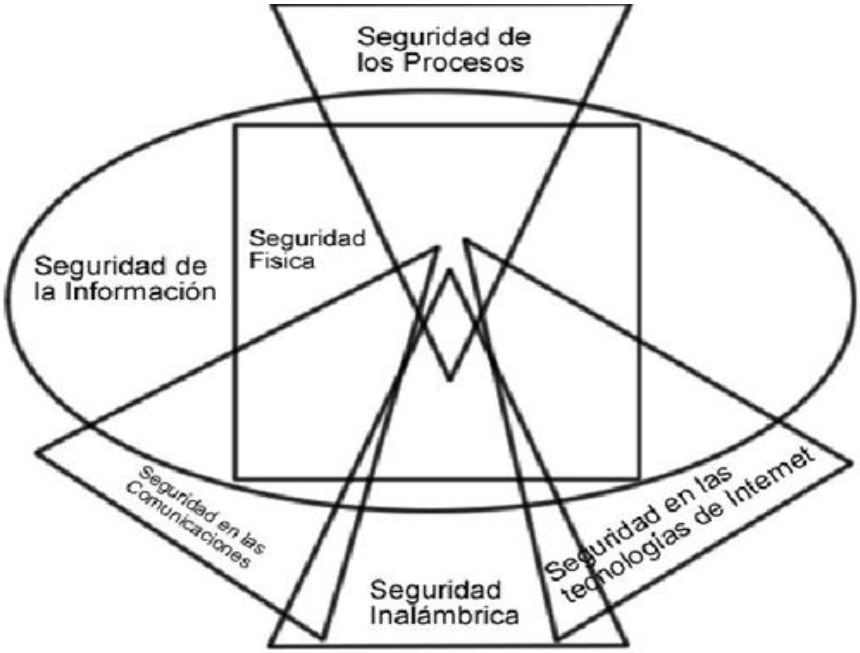

Figura 1. 1: Relación entre las distintas secciones de seguridad.

Conclusiones

En este capitulo quedan expuestos algunos conceptos útiles para un mejor entendimiento de la investigación, por lo que se explica en que consiste los test de penetración y el campo de acción en que se desenvuelve. Se hace una reseña general de la evolución de la seguridad informática, así como contenidos afines con el funcionamiento de esta rama, además de elementos afines a la relación entre un auditor de seguridad y una organización, dentro de los cuales se explica en que consiste cada uno de sus funciones y obligaciones. También se aborda la importancia que implica aplicar un test de penetración.

2

Capítulo 2 Descripción de las Pruebas.

Introducción

En este capitulo se realiza la descripción de las pruebas. La particularidad más notable de estas pruebas es que estarán guiadas mayoritariamente por los estándares que plantea la metodología OSSTMM. Como solución se propone la descripción de varias auditorias que en su conjunto van a constituir un test de penetración en la red donde se aplican, el objetivo de la aplicación de dicha pruebas se va centrar en poder demostrar la posibilidad de contribuir a mejorar la mayoría de los sectores en donde se apliquen. Una auditoria es un conjunto de pasos a seguir para obtener un conjunto de datos que delatan el estado del sistema auditado. La particularidad de estas pruebas es que son en su mayor parte genéricas ya que no describen las herramientas a utilizar, tampoco el sistema operativo usado como plataforma para desarrollar los test, solo son descritos el conjunto de pasos para alcanzar el objetivo de la auditoria y en algunos casos los resultados esperados una vez que la misma concluya.

2.1 Auditoria de Seguridad Informática.

El término de Auditoria es empleado incorrectamente con frecuencia ya que se considera como una evaluación cuyo único fin es detectar errores y señalar fallas. El concepto de auditoria es mucho más amplio. Es un análisis crítico que se realiza con el fin de evaluar y mejorar la eficacia y eficiencia de un proceso, de un departamento, un organismo u entidad. Con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, los recursos de IT (siglas en ingles de tecnologías de la información) deben ser administrados por un conjunto de procesos de IT agrupados de forma tal de obtener un modelo de referencia a implementar.

Como el campo de acción de la Auditoria informática es muy amplio, se efectúan distintos tipos de auditorias con el fin de cubrirlo en su totalidad puntualizando y profundizando cada área, departamento, organización o proceso bajo estudio, adoptando el modelo de referencia o las normas que correspondan a cada caso en estudio.

Cuando hablamos de seguridad la mayoría de las personas automáticamente asocian este término frente a ataques externos a la empresa. Se limitan a investigar la seguridad en la periferia de la empresa, que tan vulnerable es la misma frente a ataques externos, ya sea por virus, hacking o phishing,. El término de Seguridad Informática es más amplio, la seguridad interna es tanto o más importante que la externa. No nos limitamos a asegurar el exterior sino que analizamos y auditamos la seguridad interna y externa. Se estima que el 70% de los ataques que sufren las empresas provienen desde el interior de la misma.

La seguridad informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos y catástrofes naturales. La seguridad lógica se refiere a la seguridad de los activos digitales, uso del software, protección de los datos, procesos, así como a los procedimientos, normas de orden y autorización de acceso de los usuarios a la información. Se elaboran "matrices de riesgo", en donde se

consideran los factores críticos de éxito, las "Amenazas" a las que está sometida y los "Impactos" que aquellas puedan causar cuando se presentan.

La decisión de realizar una Auditoria Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Es esencial para una organización identificar sus requerimientos en materia de seguridad. Existen tres recursos principales para lograrlo.

El primer recurso consiste en evaluar los riesgos que enfrenta la organización. Mediante la evaluación de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia, y por ultimo se estima el impacto potencial. El segundo recurso está constituido por los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios. El tercer recurso es el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones. [21]

2.1.1 Auditoria de Seguridad de Sistemas Operativos y Componentes de Red.

Se analizarán y cuantificarán las vulnerabilidades encontradas en los sistemas operativos y componentes de red. Se estudiarán las políticas de seguridad implementadas, los responsables designados para el mantenimiento de los mismos. Se evaluará si los sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas. Se revisarán los parámetros variables de las Librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el desarrollador.

2.1.2 Auditoria del Impacto de los Riesgos de la Seguridad Informática.

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. La evaluación de riesgos es una consideración sistemática de los siguientes puntos:

Impacto potencial de una falla de seguridad en los negocios, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos.

Probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes de la seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos.

Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse acabo en varias ocasiones, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

Es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados a fin de:

Reflejar los cambios en los requerimientos y prioridades de la empresa.

Considerar nuevas amenazas y vulnerabilidades.

Corroborar que los controles siguen siendo eficaces y apropiados.

Las revisiones deben llevarse a cabo con diferentes niveles de profundidad según los resultados de evaluaciones anteriores y los niveles variables de riesgo que la gerencia está dispuesta a aceptar. Frecuentemente, las evaluaciones de riesgos se realizan primero en un nivel alto, a fin de priorizar recursos en áreas de alto riesgo y posteriormente en un nivel más detallado, con el objetivo de abordar riesgos específicos. [21]

2.1.3 Auditoria de Aplicaciones.

Se basa en la observación y el análisis de cuatro grandes áreas:

a) Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
b) Control Interno de las Aplicaciones: se revisan las fases que presuntamente han debido seguir en el área correspondiente de Desarrollo:

   - ❖ Estudio de Viabilidad de la Aplicación.
   - ❖ Definición Lógica de la Aplicación. Se analizará que se han observado los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto.
   - ❖ Desarrollo Técnico de la Aplicación. Se verificará que éste sea ordenado y correcto. Cuales fueron las herramientas y técnicas utilizadas en desarrollo de la aplicación.
   - ❖ Diseño del Sistema.
   - ❖ Métodos de Pruebas (Testing). Se evaluara si existe un documento de testing y como fueron ejecutadas de acuerdo a las Normas adoptas.
   - ❖ Documentación.
   - ❖ Equipo de Programación.

c) Satisfacción de usuarios: Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó.
d) Control de Procesos y Ejecuciones de Programas Críticos: Separación de ambientes. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran pueden provocar, altos costos de mantenimiento, fraudes, acciones de sabotaje, espionaje industrial-informativo, etc. Se analizara si existe separación de ambientes, personal responsable de los mismos, etc. [21]

2.1.4 Auditoria Forense.

La auditoria forense es una metodología de estudio apta para el análisis a posteriori de incidentes, mediante la cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados y se determinan los controles a implementar. [21]

2.1.5 Auditoria de Control Interno y Monitoreo.

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control. Este dominio también advierte a la Administración sobre la necesidad de asegurar procesos de control independientes, los cuales son provistos por auditorias internos y externos u obtenidos de fuentes alternativas. [21]

2.1.6 Auditoria de Adquisición e Implementación.

Las soluciones de IT deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes, para asegurar que el ciclo de vida sea continuo para esos sistemas. Esta auditoria hace hincapié en el análisis del desarrollo de las etapas mencionadas anteriormente, al grado de cumplimiento y a la segregación de funciones que debe existir en la empresa para el aseguramiento del éxito en la misma. [21]

2.1.7 Auditoria de Comunicaciones.

El objetivo de esta auditoria es evaluar los sistemas de comunicaciones de la compañía analizando los índices de utilización de las líneas contratadas, trafico de la mismas, índices pactados en los contratos, etc. La empresa deberá contar con la topología de la Red de Comunicaciones, actualizada. Se estudiarán las disfunciones organizativas, roles y encargados del cumplimiento y del mantenimiento de los servicios de comunicaciones de la empresa auditada. [21]

2.2 Tipología de test.

Blind: El auditor no tiene conocimiento previo de las defensas, los activos o canales del objetivo. Los responsables del objetivo son informados de la ejecución del test de intrusión. La profundidad de este tipo de test dependen del las habilidades y conocimientos del auditor.

Double Blind / Black box: El auditor no tiene conocimiento previo de las defensas, los activos o canales del objetivo.Los responsables del objetivo no son informados de la ejecución del test de intrusión. Permite la validación de la preparación frente a circunstancias adversas no previstas.

Gray Box: El auditor tiene conocimiento previo limitado sobre las defensas y los activos del objetivo, adicionalmente tiene conocimiento completo de los canales. Los responsables del objetivo conocen todos los detalles del test. La profundidad del test dependerá de tanto de las habilidades del auditor como de la información proporcionada por el objetivo.

Double Gray Box / White Box: El auditor tiene conocimiento previo limitado sobre las defensas y los activos del objetivo, adicionalmente tiene conocimiento completo de los canales. Los responsables del objetivo son informados del alcance y el periodo del test pero no de los canales y vectores de ataque que serán utilizados. Permite la validación de la preparación frente a circunstancias adversas no previstas.

Tandem / Crystal Box: El auditor y los responsables del objetivo tienen todos los detalles de los sistemas de información y de las pruebas. Este tipo de test comprueba la eficacia de las medidas de protección y control implantadas (p.ej. el auditor puede solicitar acceso a log, alarmas, etc.).

Reversal: El auditor tiene conocimiento detallado sobre el objetivo. Los responsables del objetivo desconocen que activos, como o cuando van a ser testeados Permite la validación de la preparación frente a circunstancias adversas no previstas. [21]

2.3 Test de Sondeo de Red.

El sondeo de red sirve como introducción a los sistemas a ser analizados. Se podría definir mejor como una combinación de recolección de datos, obtención de información y política de control. A pesar que a menudo es recomendable desde un punto de vista legal el definir exactamente y contractualmente los

sistemas a analizar si usted es un auditor externo o aun si es el administrador de sistemas, puede ser que no pueda empezar con los nombres de sistema o IPS en concreto. En ese caso es necesario sondear y analizar. La clave es encontrar el número de sistemas alcanzables que deben ser analizados, sin exceder los limites legales de lo que se quiere analizar. Por lo tanto, el sondeo de red es simplemente una forma de empezar un test; otra forma sería recibir el rango de direcciones IP a comprobar. En este módulo, no se realiza ningún tipo de intrusión directamente en los sistemas, excepto en los sitios considerados un dominio cuasi-público.

A pesar de no ser realmente un módulo en la metodología, el sondeo de red es un punto de partida. Muy a menudo se detectan más hosts durante el test. Hay que tener en cuenta que los hosts descubiertos posteriormente pueden ser añadidos en las pruebas como un subconjunto de los sistemas definidos y a menudo solamente con el permiso o colaboración del equipo de seguridad interna de la organización a analizar. [21]

Resultados esperados:

- Nombres de Dominio.
- Nombres de Servidores.
- Direcciones IP.
- Mapa de Red.
- Información ISP / ASP.
- Propietarios del Sistema y del Servicio.
- Posibles limitaciones del test.

2.3.1 Logística y Controles.

El propósito de este módulo es reducir los falsos positivos y negativos realizando los ajustes necesarios en las herramientas de análisis. [21]

Resultados esperados:

- Discrepancias por el Ancho de Banda usado en el Testeo.

- Paquetes TCP perdidos.
- Paquetes UDP perdidos.
- Paquetes ICMP perdidos.
- Problemas de enrutamiento.
- Trafico de Enrutamiento del ISP y Vendedores de Tráfico.

2.3.2 Comprobaciones de Error.

- Examinar la ruta a la red objetivo en busca de paquetes TCP perdidos.
- Examinar la ruta a la red objetivo en busca de paquetes UDP perdidos.
- Examinar la ruta a la red objetivo en busca de paquetes ICMP perdidos.
- Medir el tiempo utilizado en el recorrido TCP de los paquetes.
- Medir la latencia TCP a través de conexiones TCP.
- Medir el porcentaje de paquetes aceptados y respondidos por la red objetivo.
- Medir la cantidad de paquetes perdidos o rechazos de conexión en la red objetivo.

2.3.3 Enrutamiento.

Las Protecciones de un Router son unas defensas que se encuentran a menudo en una red donde se restringe el flujo del tráfico entre la red de la empresa e Internet. Opera en una política de seguridad y usa ACL's (Access Control Lists o Lista de Control de Acceso) que acepta o deniega paquetes. Este módulo está diseñado para asegurar que solo aquello que debe ser expresamente permitido, puede ser aceptado en la red; todo lo demás debe ser denegado. La protección también debe estar diseñada para restringir el flujo de salida de ciertos tipos de tráfico. Los Router están siendo cada vez más complejos y algunos tienen propiedades desconocidas para el auditor y a veces para la organización auditada. El papel del auditor es en parte determinar la función del router dentro de la DMZ. [21]

Resultados Esperados:

- Tipo de Router y Propiedades implementadas.
- Información del router como servicio y como sistema.
- Perfil de la política de seguridad de una red a partir de la ACL.

- Lista de los tipos de paquetes que deben entrar en la red.
- Mapa de las respuestas del router a varios tipos de tráfico.
- Lista de los sistemas vivos encontrados.

El Router y sus características:

1. Verificar el tipo de router con información reunida de la obtención de Inteligencia.
2. Verificar si el router está dando servicio de traducción de direcciones de red (NAT).
3. Verificar las intrusiones con opciones TTL estratégicas en los paquetes, (Firewalking) hecho en el módulo de escaneo de puertos.
4. Verificar la configuración de las ACL's del router
5. Testear la ACL del router en contra de las políticas de seguridad y en contra de la regla "Deny All".
6. Verificar si el router está filtrando el tráfico de la red local hacia afuera.
7. Verificar que el router esté haciendo detección de direcciones falsas.
8. Verificar las intrusiones desde un escaneo inverso en el módulo de escaneo de puertos.
9. Testear las capacidades externas del router desde el interior.
10. Cuantificar la habilidad que tiene el router para manejar fragmentos de paquetes muy pequeños.
11. Cuantificar la habilidad del router para manejar paquetes grandes.
12. Cuantificar la habilidad del router para manejar fragmentos coincidentes como los usados en ataques del tipo TEARDROP.

2.3.4 Seguridad Internet.

Objetivo: esquema de red, servicios, etc.

En una primera fase el objetivo consiste en identificar los sistemas y servicios de la organización objetivo.

2.3.5 Escaneo de red.

- Identificar el número de sistemas accesibles desde la red.
- Examinar la información registrada en los servidores de dominio.
- Identificar la parte externa de la red (traceroute).ocultos.

- Examinar las cabeceras de los correos electrónicos (correos devueltos, recibos, etc.).
- Buscar en webs de trabajo ofertas de empleo de la organización que detallen los requisitos de conocimiento de Software o Hardware específico. [21]

2.3.6 Escaneo de puertos.

- Validación activa de los puertos abiertos/filtrados de los diferentes sistemas.
- Realizar escaneo de puertos completo o parcial (Ej. 21, 22, 25, 80 y 443) para los sistemas de la red.

2.3.7 Identificación del sistema y los servicios.

- Determinar el sistema operativo y la versión del mismo (fingerprinting).
- Uso de herramientas específicas (p.ej. nmap).
- Identificación del sistema y los servicios.

2.4 Búsqueda y verificación de vulnerabilidades.

Identificar las debilidades, configuraciones inseguras y vulnerabilidades de los sistemas. En este paso se pueden utilizar herramientas automáticas, cuyos resultados deben ser acompañados de verificaciones manuales para eliminar falsos positivos. Identificar vulnerabilidades relacionadas con las aplicaciones y el sistema operativo. Verificar falsos positivos y falsos negativos.La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas. Aunque muchos escáneres automáticos están actualmente tanto en el mercado como en el mundo underground, es importante para los auditores identificar e incorporar en las pruebas que realizan los scripts y exploits que existen actualmente en el mundo underground. No obstante, es necesaria la verificación manual para eliminar falsos positivos, expandir el ámbito de hacking y descubrir el flujo de datos de entrada y salida de la red. La búsqueda manual de vulnerabilidades hace referencia a las personas que delante del ordenador utilizan la creatividad, la experiencia y la ingenuidad para probar la red objetivo. [21]

- Resultados Esperados:
- Tipo de aplicación o servicio por vulnerabilidad
- Niveles de parches de los sistemas y aplicaciones

- Listado de posibles vulnerabilidades de denegación de servicio
- Listado de áreas seguras a través de ocultación o acceso visible
- Listado de vulnerabilidades actuales eliminando falsos positivos
- Listado de sistemas internos o en la DMZ
- Listado de convenciones para direcciones de e-mail, nombres de servidores, etc.
- Mapa de red
- Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.
- Medir la organización objetivo utilizando herramientas de escaneo habituales actualmente.
- Intentar determinar vulnerabilidades por tipo de aplicación y sistema.
- Intentar ajustar vulnerabilidades a servicios.
- Intentar determinar el tipo de aplicación y servicio por vulnerabilidad.
- Realizar pruebas redundantes al menos con 2 escáneres automáticos de vulnerabilidades.
- Identificar todas las vulnerabilidades relativas a las aplicaciones.
- Identificar todas las vulnerabilidades relativas a los sistemas operativos.
- Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar a los sistemas objetivos.
- Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos.
- Verificar todos los positivos (Se debe tener en cuenta el contrato firmado con la organización objetivo en el caso de estar intentando penetrar o si se puede llegar a provocar una denegación de servicio).

2.5 Seguridad de las redes inalámbricas.

Este es un método para la verificación del acceso a redes WLAN 802.11, las cuales se están popularizando cada vez más. Sin embargo existen algunos problemas bastante comunes y alarmantes en la implantación de estas tecnologías. Se debe principalmente a que estas redes se crean rápida y fácilmente pero las medidas de seguridad no forman parte de la configuración por defecto. Existen algunas medidas básicas para mejorar la seguridad y algunas más drásticas a aplicar para conseguir unas WLANs bastante seguras. [21]

Implementaciones:

802.11a

- Opera en el rango de frecuencias de 5Ghz.
- Incompatibilidad con equipamiento 802.11b o 802.11g.
- Máxima velocidad de 54MBps.

802.11b

- Opera en el rango de frecuencias de 2.4Ghz.
- Es la tecnología más extendida actualmente.
- Máxima velocidad de 11Mbps.

802.11g

- Opera en el rango de frecuencias de 2.4Ghz.
- Máxima velocidad estándar de 54MBps.
- Se espera compatibilidad con equipamiento 802.11b existente.

Resultados Esperados:

1. Verificar que la organización disponga de una adecuada política de seguridad en uso que trate la utilización de tecnologías inalámbricas, incluyendo el uso de 802.11
2. Evaluar Equipamiento, Firmware y Actualizaciones.
3. Realizar un inventario completo de todos los dispositivos inalámbricos de la red.
4. Evaluar el Control de Acceso, Seguridad Perimetral y Habilidad para Interceptar o Interferir las
5. Comunicaciones:
6. Determinar el nivel de control de acceso físico a los puntos de acceso y dispositivos que los controlan (cerrojos, lectores de tarjetas, cámaras...).
7. Evaluar el Acceso Administrativo a los Dispositivos Inalámbricos:
8. Determinar si los puntos de acceso son apagados durante los momentos del día en los que no son

utilizados.

9. Evaluar la Configuración, Autenticación y Cifrado de las Redes Inalámbricas:
10. Verificar el cambio de los 'Service Set Identifier' (SSID) por defecto de los puntos de acceso.
11. Evaluar los Clientes Inalámbricos:
12. Verificar que todos los clientes inalámbricos poseen un antivirus instalado.

2.5.1 Seguridad física.

- Revisión perimetral.
- Mapa físico del perímetro.
- Medidas de protección (puertas, vallas, etc.).
- Rutas o métodos de acceso.
- Áreas no monitorizadas.

2.5.2 Controles de acceso.

- Enumerar las áreas con controles de acceso.
- Examinar los dispositivos de acceso y los tipos de alarmas.
- Prueba de los dispositivos de acceso para comprobar posibles limitaciones, debilidades y denegaciones de servicio.
- Revisión de las respuestas ante alarmas.
- Enumerar los dispositivos de alarma.
- Evaluar los procedimientos definidos para cada tipo de alarma.
- Prueba de los dispositivos de alarma para comprobar posibles limitaciones, debilidades y denegaciones de servicio.
- Revisión de la ubicación.
- Enumerar áreas visibles dentro de la organización.
- Enumerar áreas que faciliten la escucha pasiva dentro de la organización.
- Evaluar los controles sobre el personal de limpieza, distribución, etc.
- Revisión del entorno.
- Evaluar las probabilidades para la ocurrencia de catástrofes naturales.
- Evaluar los procedimientos de restauración y recuperación definidos. [21]

2.6 Test de aplicaciones Web.

- Búsqueda y verificación de vulnerabilidades Web.
- Las aplicaciones web a medida disponen de sus propias vulnerabilidades.
- Se requiere escaneos que identifiquen debilidades genéricas (XSS, SQL Injection, etc.) o ejecución de pruebas manuales. [21]

2.6.1 Autenticación.

Identificar los posibles accesos a la web donde pueda ser aplicados ataques de fuerza bruta (contraseñas) Buscar credenciales de acceso válidos a partir de búsquedas en el código HTML, google hacking, etc. * Consultar apartado de Seguridad de la Información. Evitar el sistema de autenticación utilizando tokens robados o falseados (p.ej. Identificadores de sesión en cookies). Identificar la lógica de la gestión de sesiones: número de reintentos fallidos de autenticación, time-outs, etc. transacción, usuario autorizado a ejecutar la transacción, etc. [21]

2.6.2 Validaciones de los datos de entrada.

Uso de números/cadenas excesivamente largos para identificar buffer overflows
Insertar en los parámetros de entrada: Comandos del sistema, SQL, LDAP, etc.
Comprobar la existencia de Cross Site Scripting (XSS).
Facilidades para la ejecución de Cross Site Request Forgeries (Session Riding).
Examinar la estructura web y el acceso a directorios no autorizados mediante path/directory transversal (p.ej. http://victima.com/download.cgi?file=../../../etc/passwd).
Utilizar diversas codificaciones de caracteres (Unicode, URL-encoded, etc.) para evitar los controles sobre los parámetros de entrada.
Manipular cookies o parámetros de formularios HTML (p.ej. hidden) para engañar o modificar la lógica de la aplicación.
Utilizar entradas ilegales o ilógicas para testear el manejo de errores de la aplicación.
Identificar mensajes de error o depuración. [21]

2.7 Testeo de Medidas de Contingencia.

Las medidas de contingencia dictan el manejo de lo atravesable, programas maliciosos y emergencias. La identificación de los mecanismos de seguridad y las políticas de respuesta que necesiten ser examinados. Debe ser necesario responder primero a una nueva cuenta de correo electrónico de pruebas o al sistema de escritorio donde el administrador pueda monitorizar. [21]

Resultados Esperados:

- Definición de las capacidades Anti -Troyano.
- Definición de las capacidades Anti -Virus.
- Identificación de las Medidas de Contingencia de Escritorio.
- Identificación de las Debilidades de Contingencia de Escritorio.

Lista de recursos de contingencia:

- Medir el mínimo de recursos necesarios que se necesitan en el subsistema para realizar las tareas.
- Verificar los recursos disponibles a este subsistema que necesiten realizar estas tareas, y que recursos están protegidos desde este subsistema.
- Verificar la detección de medidas presentes para la detección de intentos de acceso a los recursos protegidos.
- Verificar recursos innecesarios.
- Verificar las propiedades del sistema de contingencia.
- Verificar la detección de medidas presentes para la detección de accesos 'no comunes' a los recursos 'necesarios'.
- Medidas de configuración del sistema.

2.8 Descifrado de Contraseñas.

Descifrar las contraseñas es el proceso de validar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas automatizadas, que dejan al descubierto la aplicación de

algoritmos criptográficos débiles, implementaciones incorrectas de algoritmos criptográficos, o contraseñas débiles debido a factores humanos. Este módulo no debe ser confundido con el de recuperación de contraseñas vía escucha de de texto por canales libres, es más sencillo de entender que un trastorno del sistema de seguridad, pero solo que tiene mecanismos de autenticación sin cifrar, nada de debilidades en contraseñas [Nota: Este módulo puede incluir técnicas para averiguar manualmente las contraseñas, que explote los usuarios y contraseñas por defecto en aplicaciones o sistemas operativos (p.ej. Usuario: System Contraseña: Test) o fácilmente predecible por parte del error de un usuario (p.ej. Usuario: joe Contraseña: joe). Este puede ser un sistema para obtener acceso a un sistema inicialmente, quizá sea siempre con acceso de administrador o root, pero solo con fines educativos. Más allá de la predictibilidad manual de las contraseñas, a través de combinaciones por defecto o simples, se puede hacer fuerza bruta de contraseñas para aplicaciones como Telnet, usando scripts o programas personalizados, al menos no es viable por valores de espera agotados, siempre con aplicaciones de fuerza bruta con multiconexión (simulando el multihilo).

Una vez entrado con privilegios de root o administrador en un sistema, el descifrado de contraseñas consiste en obtener acceso a sistemas o aplicaciones adicionales (gracias a los usuarios cuyas contraseñas sean coincidentes en múltiples sistemas) y es una técnica válida que puede ser usada por influencia del sistema a través de un test de seguridad. Descifrados de contraseñas minuciosos pueden ser realizados como un ejercicio de simple y debe ser subrayada la necesidad de algoritmos criptográficos fuertes para contraseñas de almacenamiento de sistemas de llave, también subrayar la necesidad del refuerzo de una política estricta de contraseñas de usuario, generación automática. [21]

Resultados Esperados:

- Ficheros de Contraseñas descifrados o no descifrados.
- Lista de cuentas, con usuario o contraseña de sistema.
- Lista de sistemas vulnerables a ataques de descifrado de contraseñas.
- Lista de archivos o documentos vulnerables a ataques de descifrado de contraseñas.
- Lista de sistemas con usuario o cuenta de sistema que usan las mismas contraseñas.

1. Obtener el fichero de contraseñas desde el sistema que guarda nombres de usuario y contraseña.

- ❖ Para sistemas Unix, ha de estar en /etc/passwd o/y /etc/shadow.
- ❖ Para sistemas Unix que tienen que realizar autenticaciones SMB, puede encontrar las contraseñas de NT en /etc/smbpasswd.
- ❖ Para sistemas NT, ha de estar en /winnt/repair/Sam. (U otra, más difícil de obtener variantes).

2. Arranque un ataque automatizado de diccionario al fichero de contraseñas.
3. Arranque un ataque de fuerza bruta al fichero de contraseñas.
4. Usar contraseñas obtenidas o sus variaciones para acceder a sistemas o aplicaciones adicionales.
5. Arranque Programas automatizados de descifrado en ficheros cifrados que haya encontrado (como documentos PDF o Word) como intento de recopilar más datos y subrayar la necesidad de un cifrado del sistema o de documentos más fuerte.
6. Verificar la edad de las contraseñas.

2.9 Testeo de Denegación de Servicios.

La Denegación de Servicios (Dos) es una situación donde una circunstancia, sea intencionada o accidental, previene el sistema de tal funcionalidad como sea destinada. En ciertos casos, el sistema debe funcionar exactamente como se diseñó, nunca fue destinado para manejar la carga, alcance, o parámetros que abusen de ellos.

Es muy importante que los test de Dos reciban ayuda adicional de la organización y sea monitorizada a nivel privado. Inundación y ataques Dos Distribuidos (DDoS) están específicamente no comprobados y prohibidos por este manual. Los ataques de inundación y los ataques DDoS SIEMPRE causarán ciertos problemas y a veces no solamente al objetivo sino también a los enrutadores y sistemas entre el auditor y el objetivo. [21]

Resultados Esperados:

- ❖ Lista de puntos débiles en presencia de Internet incluidos los puntos individuales por averías.
- ❖ Establecer un punto de referencia para un uso normal.

- Lista de comportamientos de sistema por un uso excesivo.
- Lista de sistemas vulnerables a Dos.

1. Verificar que las cuentas administrativas y los archivos y recursos de los sistemas están asegurados apropiadamente y todos los accesos están concedidos con "Mínimo Privilegio".
2. Comprobar las restricciones de sistemas expuestas a redes sin confianza.
3. Verificar que los puntos de referencia están establecidos a partir de una actividad normal del sistema.
4. Verificar que los procedimientos están en un lugar que responde a una actividad irregular.
5. Verificar la respuesta a una información negativa SIMULADA (ataques propaganda).
6. Testear cargas de red y de servidor excesivas.

2.10 Evaluación de Políticas de Seguridad.

La política de seguridad resaltada aquí es el documento escrito legible que contiene las políticas que delinean la reducción de riesgos en una organización con la utilización de tipos específicos de tecnologías. Esta política de seguridad puede ser también una forma legible de Listas de Controles de Acceso. Existen dos funciones a llevar a cabo: primero, el testeo de lo escrito contra el estado actual de las conexiones de la presencia en Internet y de otras conexiones no relacionadas a Internet; y segundo, asegurar que la política este incluida dentro de las justificaciones de negocio de la organización, y de los estatutos legales locales, federales e internacionales, en especial en referencia a los derechos y responsabilidades tanto del empleador como de los empleados y la ética de privacidad personal.

Esta tareas exigen que el testeo y verificación de vulnerabilidades sea hecho en su totalidad y que todas las otras revisiones técnicas hayan sido llevadas a cabo. A menos que esto sea realizado, no es posible comparar los resultados con los lineamientos a lograr especificados por las políticas de seguridad, traducidos en medidas de protección del entorno operativo. [21]

1. Comparar la política de seguridad contra el estado actual de la presencia en Internet.
2. Aprobación de la Gerencia – Busque cualquier signo que revele que la política está aprobada por la gerencia. Sin esta aprobación, la política no tiene valor porque el personal no tiene la obligación de seguir las reglas establecidas en la política. Desde un punto de vista formal, UD puede detener las investigaciones de la política de seguridad si ésta no es aprobada por la gerencia. Sin embargo, el

testeo debería continuar para determinar cuán efectivas son las medidas de seguridad en el estado actual de la presencia en Internet.

3. Cerciórese de que la documentación está adecuadamente almacenada, ya sea electrónicamente o en otros medios, y que la política ha sido leída y aceptada por el personal incluso antes de que ellos obtengan acceso a los sistemas informáticos.
4. Identifique los procedimientos de manejo de incidentes, para asegurarse de que las brechas de seguridad son manejadas por las personas adecuadas y que son reportadas de manera apropiada.
5. Conexiones entrantes – Verifique los riesgos mencionados que tienen relación directa con las conexiones entrantes de Internet (Internet -> DMZ, Internet -> red interna), y las medidas que son necesarias implementar para reducir o eliminar dichos riesgos. Estos riesgos pueden ser permitidos en conexiones entrantes, típicamente SMTP, POP3, HTTP, HTTPS, FTP, VPNs y las correspondientes medidas como esquemas de autenticación, encriptación y Listas de Control de Acceso. Específicamente, las reglas que niegan el acceso con estado a la red interna generalmente no son alcanzadas por la implementación.
6. Conexiones salientes – Las conexiones salientes pueden producirse entre la red interna y DMZ, así como también entre la red interna e Internet. Busque cualquier regla de conexiones salientes que no se corresponda con la implementación.
7. Las conexiones salientes no pueden ser usadas para introducir código malicioso o revelar las especificaciones de la red interna.
8. Medidas de seguridad – Las reglas que exigen la implementación de medidas de seguridad, deben ser cumplidas.
9. Aquellas pueden hacer uso de AVS, IDS, cortafuegos, DMZs, routers y las configuraciones/implementaciones adecuadas de acuerdo con los riesgos a contrarrestar.
10. Comprobar la política de seguridad contra el estado actual de las conexiones no relacionadas a Internet.
11. Módems – Debe existir una regla que indique que el uso de módems que no están especialmente asegurados está prohibido o al menos sólo permitido si los módems están desconectados cuando no se encuentran en uso, y configurados para no permitir el marcado. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.

12. Máquinas de Fax – Debe existir una regla que indique que el uso de las máquinas de fax que pudiera permitir acceso desde el exterior a la memoria de las máquinas, está prohibido o al menos sólo permitido si las máquinas son apagadas cuando no se las utiliza. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.
13. PBX – Debe existir una regla que indique que la administración remota del sistema PBX está prohibida o al menos sólo permitida si las máquinas son apagadas cuando no se las utiliza. Verifique tanto si la regla correspondiente existe como si la implementación sigue los requisitos.
14. Verifique que la política de seguridad establezca las medidas de contención y los test de ingeniería social basados en el uso indebido de Internet por parte de los usuarios, de acuerdo con la justificación de negocios y las mejores prácticas de seguridad.

Conclusiones

Abordamos en este capitulo el contenido y descripción de una gran cantidad de pruebas de penetración, las cuales se detallan minuciosamente. De esta descripción detallada se logra obtener una referencia profunda de cómo están estructuradas estas pruebas, los pasos a seguir para la realización de las mismas y algunos resultados esperados cuando estas sean ejecutadas. Aunque no están documentadas todos los test si se encuentran los que se consideraban mas útiles e importantes para el centro. Para describir estas pruebas se selecciona el manual de metodología abierta OSSTMM ya que en una primera fase de implementación de medidas de seguridad en entornos que no reciben mucha atención en este sentido, por su facilidad de implementación de lo que propone este manual es un punto de partida idóneo para implementar niveles de seguridad adecuados en los lugares en donde se apliquen las pruebas. Con esto no se quiere demostrar que una metodología es mejor que otra sino que desde un punto de vista de implementación de seguridad escalonada es un excelente comienzo usar esta metodología.

3

Capítulo 3 Implementación.

Introducción

En este capitulo se abordaran una serie de pruebas que se realizan con un conjunto de herramientas especializadas las cuales tienen como resultado una salida de datos los cuales pueden ser utilizados para identificar el estado de las estructuras analizadas. Esta serie de datos deben ser cuidadosamente estudiados para detectar los tipos de vulnerabilidades que puedan tener las estructuras analizadas, después de esta serie de pasos y según los resultados obtenidos se puede estructurar una conjunto de recomendaciones que contribuyan a minimizar estas vulnerabilidades. Por comodidad y ahorro de tiempo en el proyecto se decide usar como plataforma de desarrollo del test el sistema operativo Windows XP ya que atrasaría más el proyecto si se tuviese que configurar un sistema de código abierto con el conjunto de herramientas necesarias para aplicar las pruebas. Las herramientas seleccionadas para la ejecución de las pruebas en muchos caso no se pueden usar las mas idóneas o las que más ofrecen datos de salidas interesantes ya que se dificulta poder lograr reunir una colección de herramientas que respondan a las necesidades del desarrollo de este proyecto.

3.1 Identificación de Banner.

Herramienta: SCANLINE [5]

Prerrequisitos: Ninguno.

Contramedidas: Desinstalar y/o deshabilitar servicios innecesarios que se ejecutan en la máquina (ejemplo: SSH, VPN, IPSEC), alteración de banners.

Descripción: SCANLINE tiene varios usos, entre ellos puede ser utilizada para obtener los banner ofrecidos por los servicios de la máquina objetivo.

Procedimiento: Descargar la herramienta y ejecutar los siguientes comandos sl –bth [puerto] [ip o rango] [ver figura 3.1]. (Solo disponible en Windows).

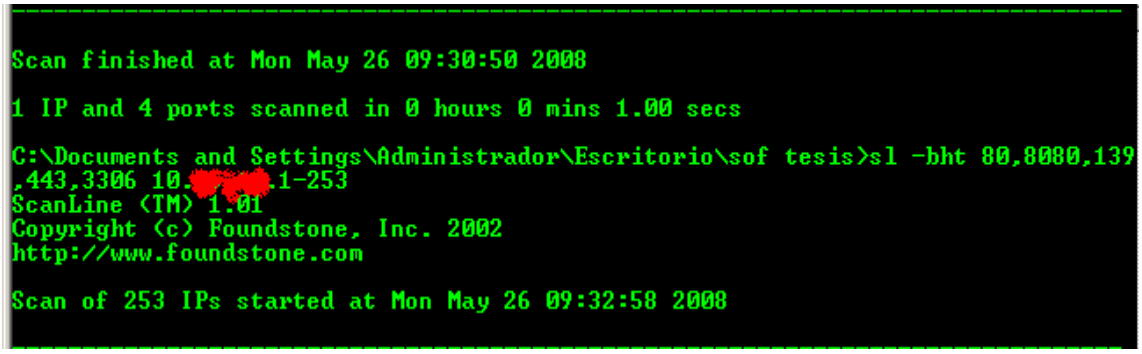

Figura 3. 1: Ejecución de comandos.

Los resultados son contundentes, nos muestra un listado completo de los servicios activos en la máquina objetivo [ver figura 3.2], además de algunas opciones de utilización, de las cuales se destaca la posibilidad de seleccionar algunos puertos TCP específicos evitándose de esta manera la alerta general de los sistemas de identificación de intrusos o de ataques.

Figura 3. 2: Servicios activos.

La enumeración de objetivos, es la actividad mediante la cual se puede obtener, recolectar y organizar la información de máquinas, redes, aplicaciones, servicios y/o otras tecnologías disponibles y ofrecidas por el o los objetivos.

Realmente no se considera un ataque, púes solo pretende recopilar de manera organizada información disponible mediante consultas [ver figura 3.3], con el fin de elaborar verdaderos ataques, basados en los resultados obtenidos mediante la enumeración.

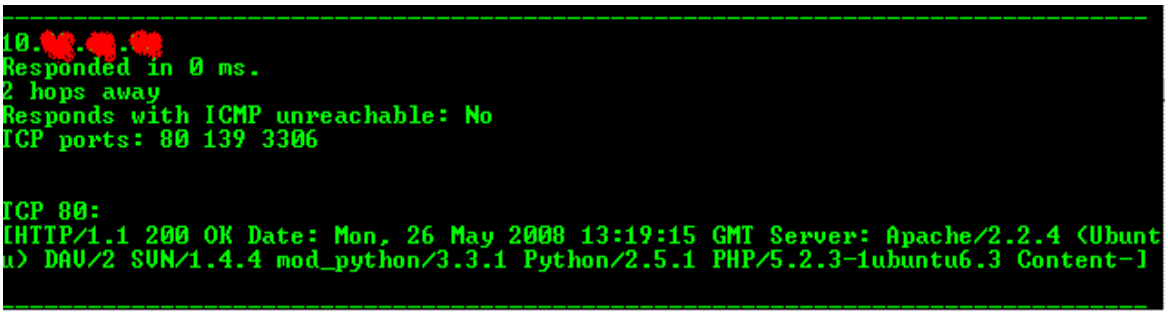

Figura 3. 3: Servicios activos.

Las herramientas y técnicas de enumeración están basadas en su mayoría en escaneos simples a la máquina objetivo, en simples peticiones o consultas.

3.2 Enumerar dirección MAC del objetivo.

Herramienta: GETMAC. [6]

Prerrequisitos: Sesión nula.

Contramedidas: Restringir conexiones anónimas, Firewalls.

Descripción: La aplicación getmac puede ser utilizada para identificar la dirección MAC (Media Access Control address) asignada a cada tarjeta de red (NIC) del objetivo. Otro de los usos de la herramienta getmac es identificar el número de tarjetas de red del objetivo [ver figura 3.4].

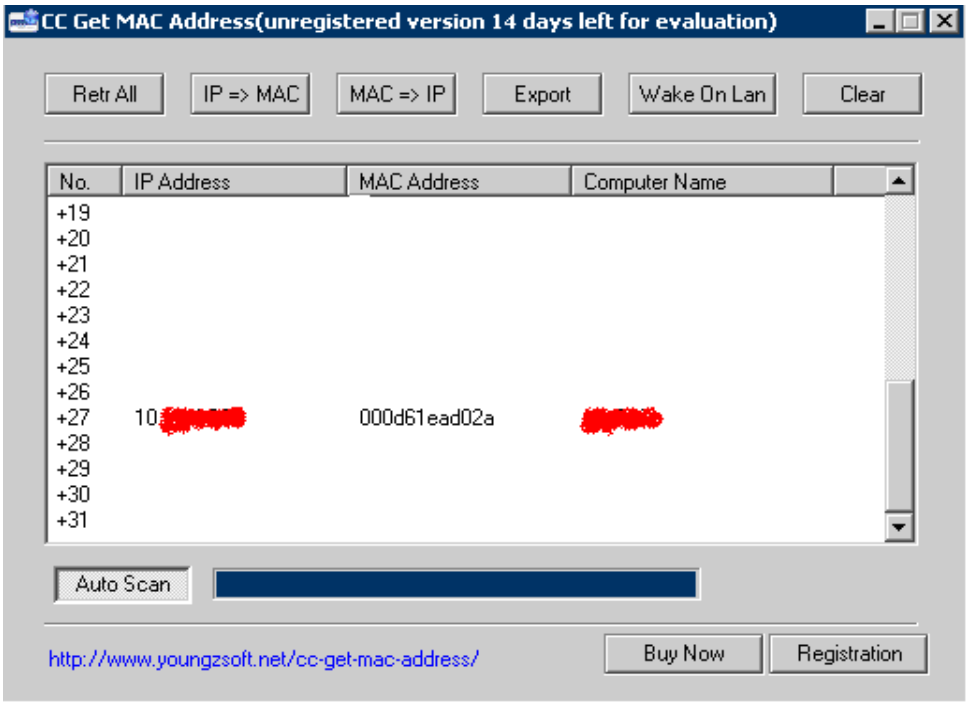

Figura 3. 4: Datos que muestra la herramienta.

Procedimiento: Descargar e instalar la herramienta, y poner una dirección IP o un rango de estas.

3.3 Detección de vulnerabilidades.

Herramienta: GFI LANguard N.S.S [7]

Prerrequisitos: Ninguno.

Contramedidas: Firewalls.

Descripción: Es un analizador de red que además de escanear puertos y servicios busca posibles agujeros de seguridad mediante escaneo, buscando faltas de parches de seguridad, recursos compartidos abiertos, cuentas de usuarios, etc. Además permite instalar los parches faltantes y service packs.

Procedimiento: Ingresar a la herramienta la dirección IP o el rango de IP's del sistema objetivo de escaneo. Ahora se selecciona una de las dos opciones que nos ofrece GFI LANguard para almacenar los resultados y generar los reportes. Microsoft ACCESS (no requiere instalación adicional) Microsoft SQL Server 2000 o superior (debemos crear la conexión ODBC y demás).

Para ejecutar la herramienta debemos completar 5 sencillos pasos de configuración de uso:

Tipo de escaneo: Se tienen 4 opciones disponibles para ejecutar un escaneo.

Escaneo de vulnerabilidades: Escaneará el sistema en busca de bugs (fallas) de seguridad almacenada en la base de datos de GFI LANguard. (Las vulnerabilidades son actualizadas mediante el proceso de upload anterior [ver figura 3.5], profundizaremos en el concepto de escaneo de vulnerabilidades en próximos laboratorios).

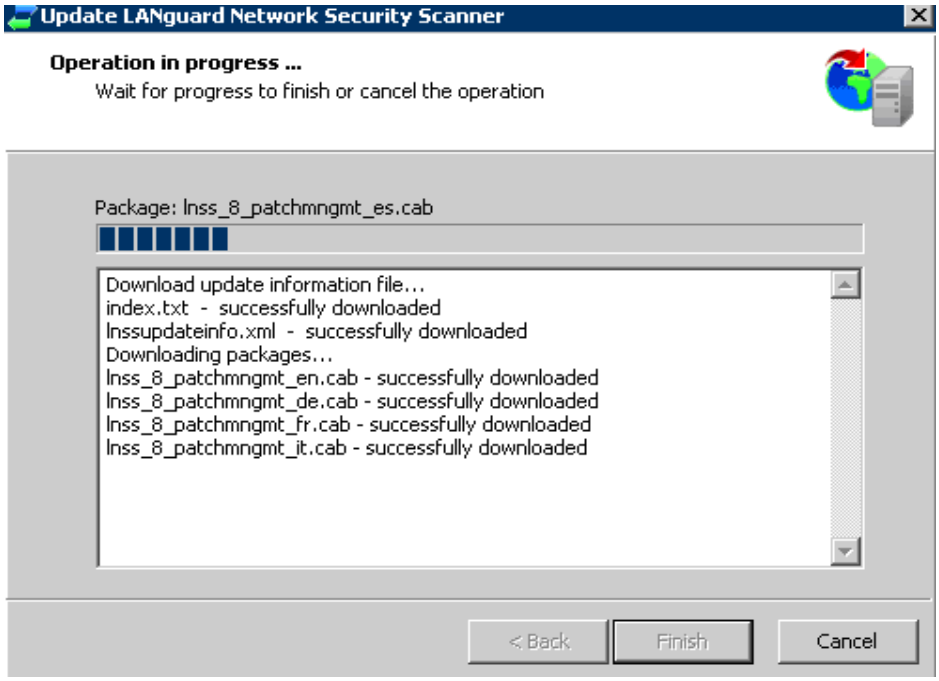

Figura 3. 5: Proceso de actualización.

Estado de parches: Mediante el escaneo permite identificar el estado actual de los parches instalados en los sistemas objetivos [ver figura 3.6].

Inventario de red y de software: Nos permite realizar completos inventarios de recursos de red y de software a las máquinas o redes objetivos así como su vulnerabilidades mas criticas [ver figura 3.7]...

Completo: Combina las tres opciones anteriores de escaneo (vulnerabilidades, parches e inventario).

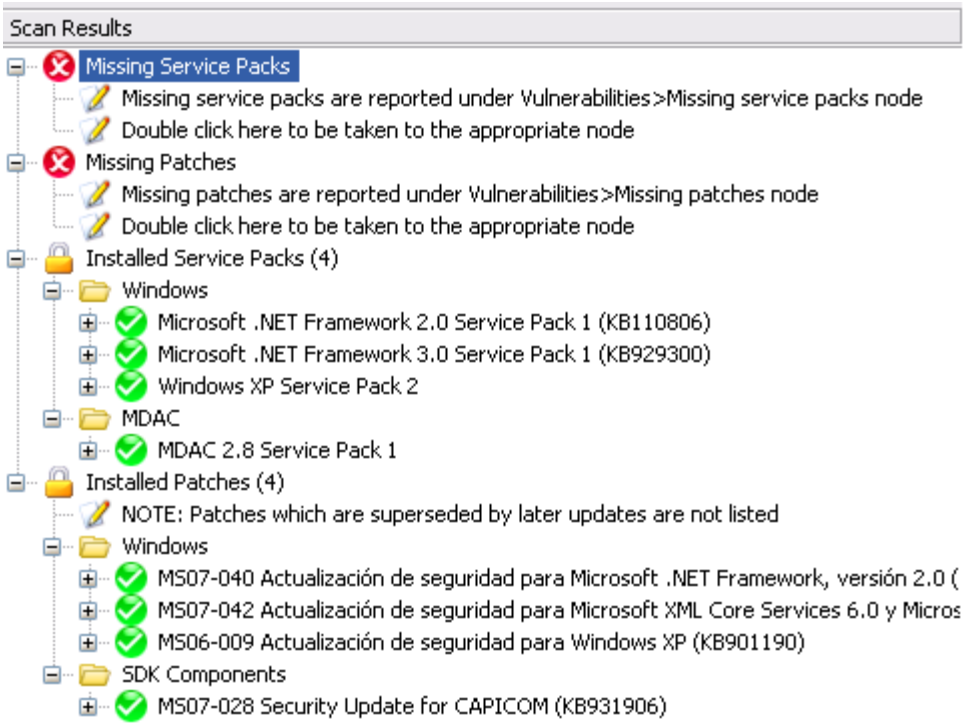

Figura 3. 6: Estado de parches instalados.

Otra opción permite realizar el escaneo haciendo uso de varios métodos de autenticación: usuario actual, otras credenciales, sesión nula, llave SSH privada

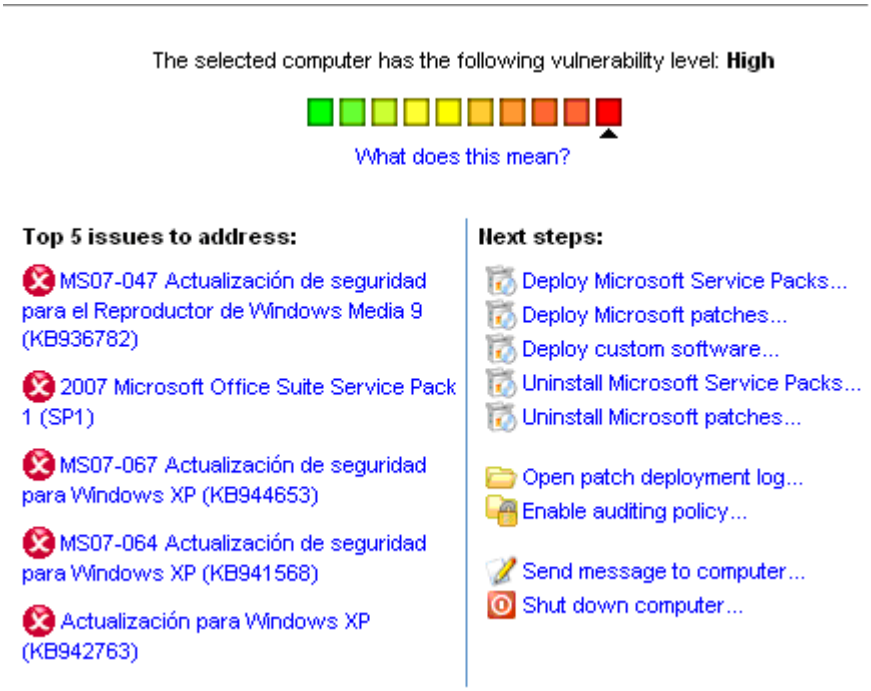

Figura 3. 7: Inventario de actualizaciones no intaladas.

MAC Address Servicios (además las versiones del software que gestionan dichos servicio), Usuarios, Recursos compartidos, Usuario autentificado actualmente, Tarjetas de red Vulnerabilidades, Parches, Service Pack, Políticas de seguridad.

Otra información de utilidad [ver figura 3.8].

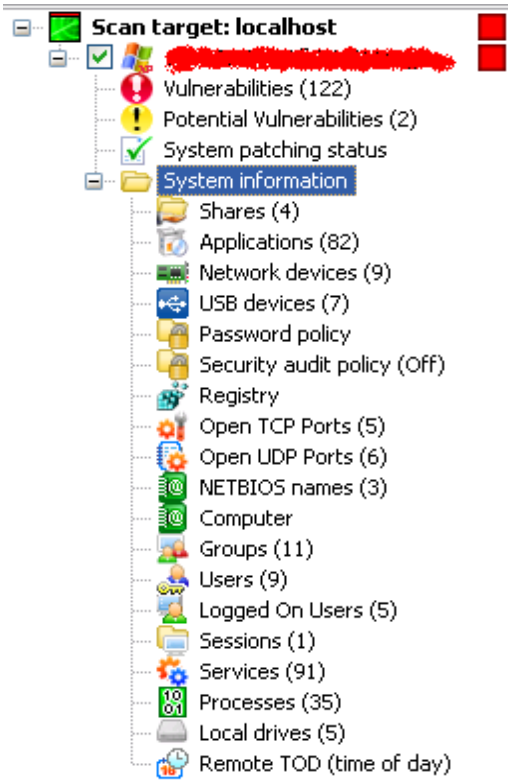

Figura 3. 8: Otra información.

3.4 Identificación del Sistema Operativo.

Herramienta: NMAP.

Prerrequisitos: Ninguno.

Contramedidas: Alteración de banners, Firewalls, Sistemas de detección de intrusos (IDS).

Descripción: Determina qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características.

La aplicación Nmap va a ser utilizada para identificar el posible S.O de la máquina objetivo. Un atacante puede utilizar esta información para llevar a cabo ataques más elaborados.

Procedimiento: Ejecutar la siguiente sintaxis:

Nmap <opciones> (Dirección IP)

Ejemplo:

nmap -sS -p 139 -O -D 24.213.28.234 192.168.146.131

La opción -sS, da la instrucción a nmap que utilice TCP sincronizado (SYN) encubierto o sigiloso, enviando un paquete SYN, sin luego enviar el paquete ACK, evitando de esta manera el establecimiento de conexión y por ende el registro en los log.

La opción -p 139 ordena a nmap dirigir su actividad (escaneo) al puerto 139.

La opción -O ordena a nmap usar TCP/IP fingerprinting para identificar el S.O de la máquina objetivo.

La opción -D 24.213.28.234 ordena a nmap usar esta IP como método encubierto, es decir, que los sistemas de detección de intrusos o los mismos log que puedan generar los intentos de identificación del S.O lanzado por nmap quedarán registrados con esta IP como dirección de inicio del “ataque”. Esta es una de las opciones más interesantes de nmap, pues permite a un atacante encubrir su verdadera identidad. Para hacer el trabajo más complicado para el administrador del sistema, el atacante puede utilizar varias IP falsas separadas por una coma (24.24.24.24, 24.24.24.25, 24.24.24.26, etc.)

Ahora se hará usode la herramienta Nmap desde un entorno Windows.

La nueva versión de nmap permite dirigir escaneos pre-establecidos, es decir, simplemente seleccionando la opción perfil, obtendremos los comandos necesarios para dirigir un “ataque”. Para el caso seleccionaremos Quick Operating System detection, pero mejoraremos la línea de comandos pre-establecida, agregando la opción señuelo -D con la IP 69.69.69.69. Veamos:

Los resultados obtenidos, tantos puertos y servicios abiertos, MAC Address y el objetivo: Sistema Operativo [ver figura 3.9 y 3.10]. [6]

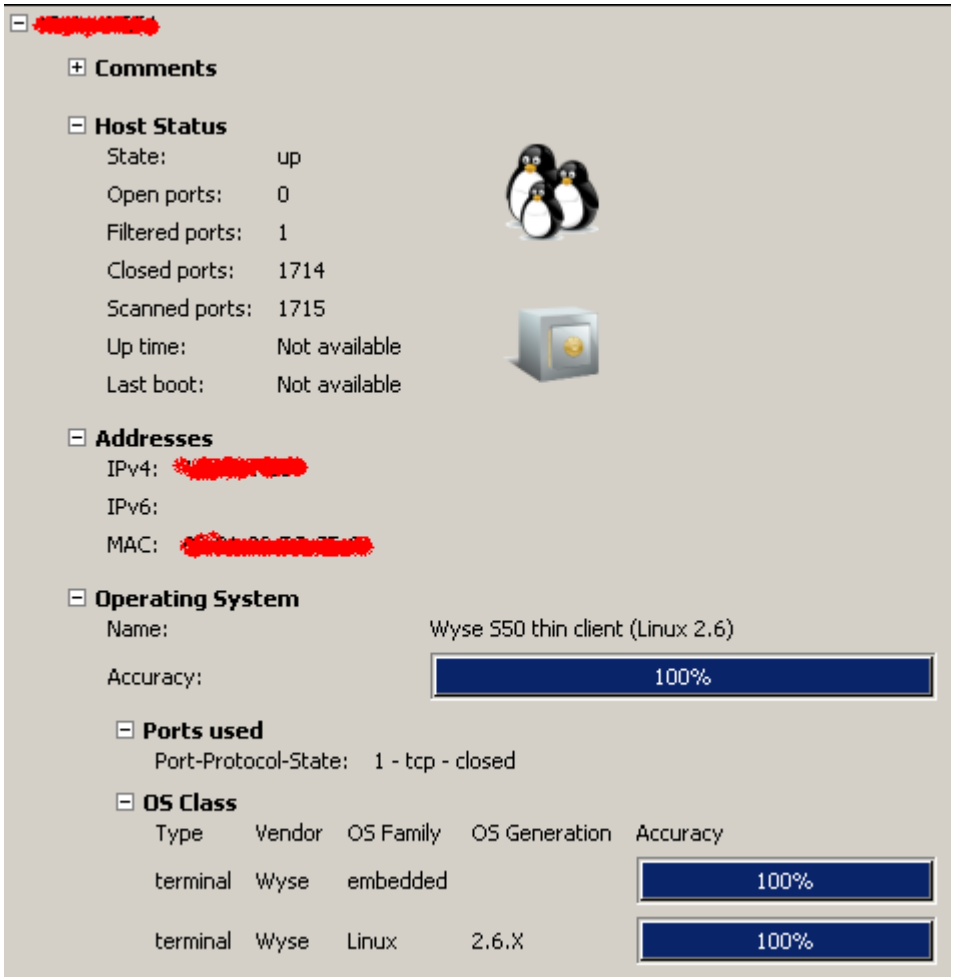

Figura 3. 9: Información obtenida.

```
Scanning             [1715 ports]
Discovered open port 3389/tcp on
Discovered open port 912/tcp on
Discovered open port 139/tcp on
Discovered open port 1025/tcp on
Discovered open port 135/tcp on
Discovered open port 445/tcp on
Completed SYN Stealth Scan at 13:28, 1.39s elapsed (1715 total ports)
Initiating OS detection (try #1) against
Host              appears to be up ... good.
Interesting ports on
Not shown: 1709 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
912/tcp  open  unknown
1025/tcp open  NFS-or-IIS
3389/tcp open  ms-term-serv
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
```

Figura 3. 10: Información obtenida.

3.5 Conectividad del objetivo.

Detectando la conectividad del objetivo con Pathping.

Prerrequisitos: Ninguno.

Contramedidas: Denegar peticiones/respuestas ECHO/ICMP en el/los routers.

Descripción: Proporciona información acerca de la latencia de red y las pérdidas de red en saltos intermedios entre un origen y un destino. Pathping envía múltiples mensajes de solicitud de eco a cada enrutador entre un origen y un destino en un período de tiempo y calcula los resultados en función de los paquetes devueltos desde cada enrutador. La mayoría de las veces las máquinas objetivos están detrás de routers, este comando ayuda a identificar los mismos. [6]

Procedimiento: Desde la Shell de Windows ejecutar la siguiente sintaxis:

pathping (Dirección IP Objetivo o nombre de host)

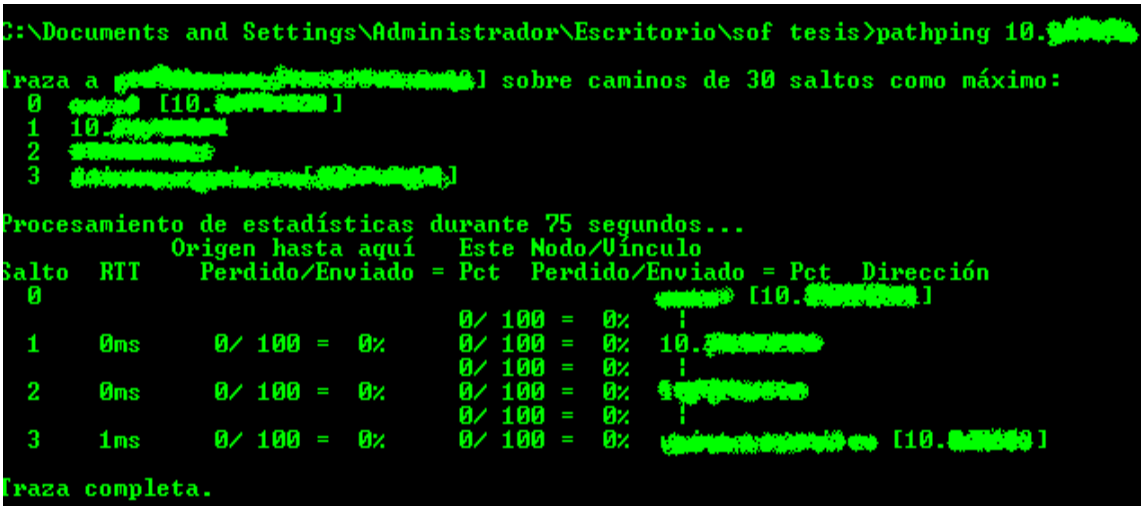

Figura 3. 11: Resusltados obtenidos.

Los resultados arrojados en esta consulta permiten conocer los saltos en cada router hasta la máquina o router objetivo. Además permite calcular las estadísticas por cada salto en cada router. Cabe recordar que en muchos de los casos en último salto es la ip perteneciente a un router. Router potencialmente propenso a ataques si se encuentra débilmente asegurado [ver figura 3.11].

3.6 Localización / Identificación de registros.

Herramienta: Visual Route. [19]

Prerrequisitos: Ninguno.

Contramedidas: Ocultar datos sensibles y/o personales en el momento de hacer registros de máquinas, dominios y/o servicios derivados.

Descripción: La aplicación Visual Route permite no solo hacer un trazado [ver figura 3.12 y 3.13] de ruta a la máquina Web objetivo, sino también ofrece un servidor geo localizador de la misma. Además de Ping test, IP Trace, Localización de IP's, DNS Lookup y más.

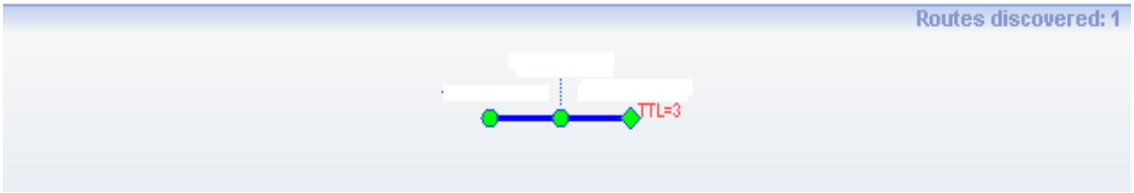

Figura 3. 12: Trazado de ruta.

Procedimiento: Descargar la versión que más se ajuste a las necesidades, existen dos opciones, una versión Lite con algunas limitaciones importantes para la información que se pretende obtener y otra versión completamente operativa.

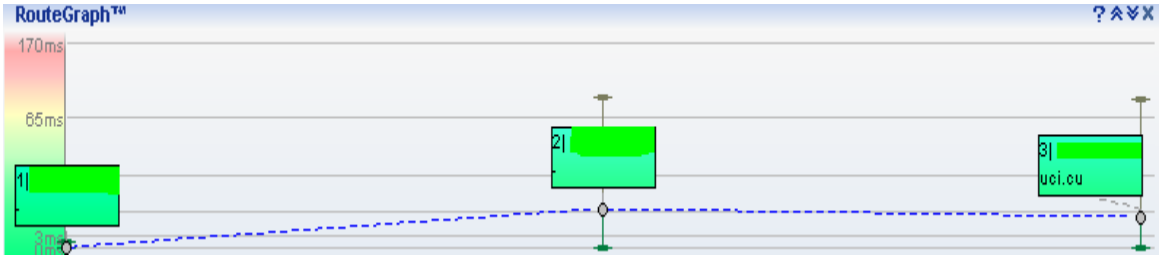

Figura 3. 13: Trazado de ruta.

3.7 Captura de paquetes. Extrayendo datos desde el tráfico de red.

Herramienta: Ethereal. [8]

Prerrequisitos: WinPcap.

Contramedidas: Encriptación Sistemas de detección de sniffers.

Descripción: Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos. Cuenta con todas las características estándar de un analizador de protocolos.

La información que puede tener un atacante (en este caso, como investigador) haciendo uso de este tipo de ataques es la siguiente:

- Direcciones IP.
- Nombres de host (Hostnames).
- Routers y rutas de transmisión.
- Datos (la mayoría de los datos transmitidos en red circulan en texto plano, incluyendo FTP, Telnet, e-mail, etc).
- Información de protocolos.

Mediante este tipo de ataques, el delincuente informático puede construir ataques más elaborados, en apoyo de los datos obtenidos por esta técnica.

Procedimiento: Instalar la herramienta wireshark. Veamos el proceso llevado a cabo en Windows:

Desde la pestaña Capture [ver figura 3.14], hacemos clic en el botón Options. Esta ventana permitirá seleccionar nuestra tarjeta de red además activaremos la opción de resolución de nombre de red. Las demás opciones se pueden dejar por defecto.

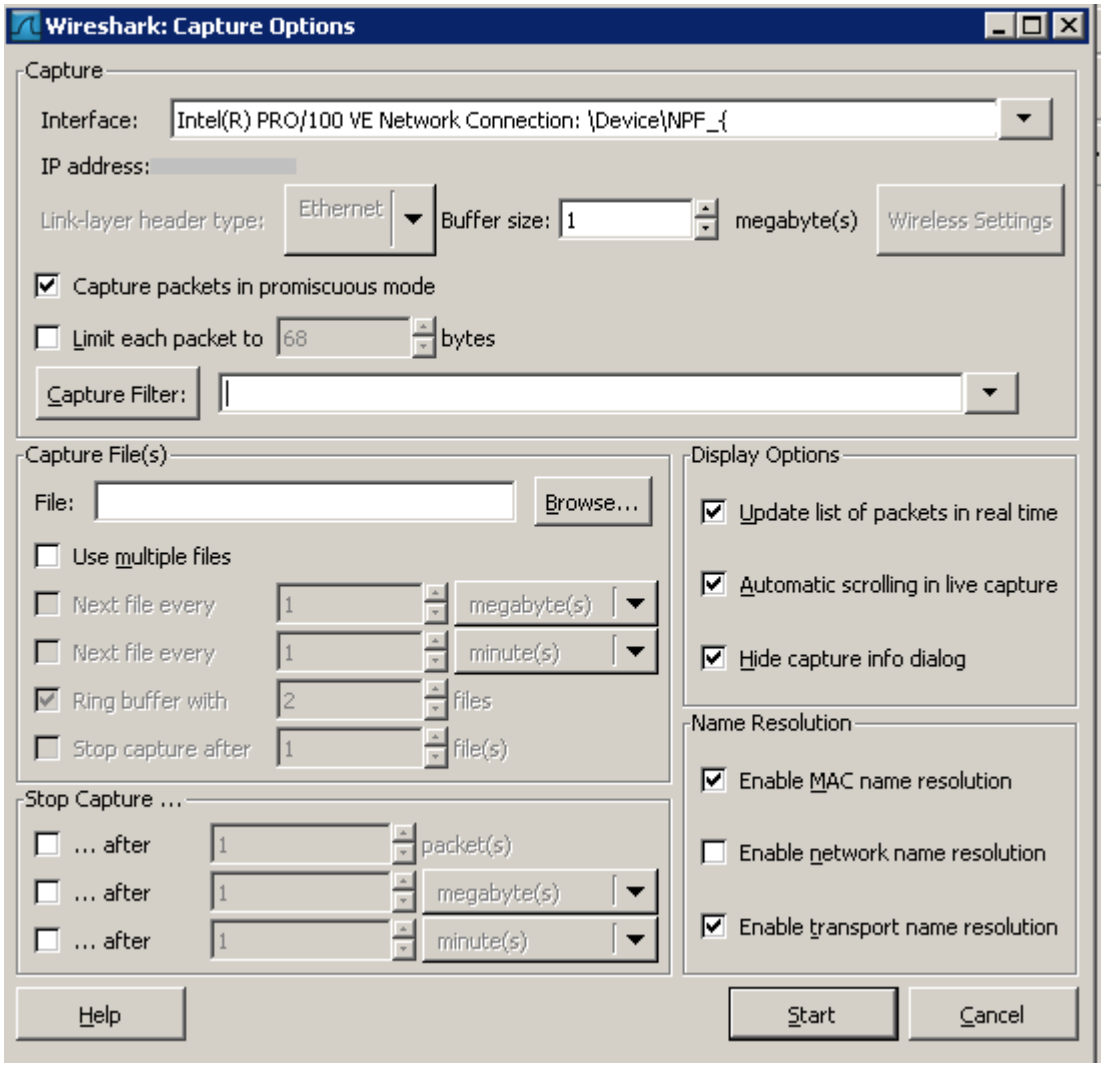

Figura 3. 14: Ventana de configuración.

Dicho esto, se da comienzo con el sniffing de tráfico [ver figura 3.15].

```
<html><head><title>Error</title></head><body>Error: Access is Denied.</body></
ntml>POLL /                    /Inbox HTTP/1.1
Accept: */*
Referer:
Subscription-id: 298033
Accept-Language: es-co
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Alexa Toolbar;
MEGAUPLOAD 2.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; WWTClient2)
Host: 10
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
Authorization: Negotiate TlRMTVNTUAABAAAAB4IIogAAAAAAAAAAAAAAAAAAAAAFASgKAAAAD0==
Cookie: sessionid=38eaf9f3-72c7-485a-892b-3774fe8e51b1:0xc0a
```

Figura 3. 15: Comienzo del sniffing.

AuthType	LM Hash	NT Hash	NT Serv-Chall	LM Cli-Chall
ClearText				
NTLM Session S...	EADBBD9D168...	DCEE70A62679...	42D165664580...	000000000000...
NTLM Session S...	60935C32BB41...	E386ED9F6C9F...	BB2452BCA97A...	000000000000...
NTLM Session S...	B2EBDAFF70B8...	F83285A9362C...	17EBC0E86653...	000000000000...
NTLM Session S...	97C3AC4D8477...	F75954799075...	F4AACB5B9DD...	000000000000...
NTLM Session S...	7C63117E580C...	D525954A0A26...	5F419ABC5202...	000000000000...
NTLM Session S...	4548EEDAC178...	72B82E004947...	DCA4E9815B5A...	000000000000...
NTLM Session S...	9B1C1543C427...	A6EEF8194AC9...	5F13FD9E3F0F...	000000000000...
NTLM Session S...	F027F900D632...	EEBA7DA81C2F...	5C5A8899E43C...	000000000000...
NTLM Session S...	E7ED133C46DB...	D15F197DBE33...	C39977F41E4D...	000000000000...
NTLM Session S...	5F92F0B7528C...	CB2A1E72819F...	3016E4965559...	000000000000...
NTLM Session S...	2875E77B7D0D...	3FE1C0B92940...	E8C357BCE388...	000000000000...
NTLM Session S...	50B1FC7A65AF...	25EF9E627B47...	9B98F342ABF9...	000000000000...
NTLM Session S...	14E8CD59645B...	4807DA6089A3...	6DBD79CC79E...	000000000000...
NTLM Session S...	062B6EE6403C...	EE46EDE31E0D...	F05DBAD75BF3...	000000000000...
NTLM Session S...	04C7DE2D4180...	F92FA855A755...	41D55FD3C28B...	000000000000...
NTLM Session S...	40BD42415C6C...	A705D9B6616A...	2264E12A5E5D...	000000000000...
NTLM Session S...	5B342E948B03...	6874523F0328...	9F9F7CC0E798...	000000000000...
NTLM Session S...	0F5EC036BB85...	2472D715CA06...	06A5A9C94294...	000000000000...
NTLM Session S...	217D190993E4...	BEDD1FCE4AFE...	B675C8C6DD80...	000000000000...
NTLM Session S...	B3794AF1AA5C...	B8A8CFD9579E...	63F9323090B6...	000000000000...

Figura 3. 16: Datos mostrados.

Captura de pantalla de la herramienta Wireshark en ejecución [ver figura 3.16], rápidamente se observa como recoge cada uno de los datos transmitidos en la red. Es una de las mejores herramientas para este propósito.

3.8 TEST Antivirus Kaspersky v6.0.2.678.

Detectan ejecución sobre UNICODE y sobre rutas largas. Detectan por contenido el tipo de fichero y no por la extensión. Además el servicio y los ficheros asociados se auto protege:

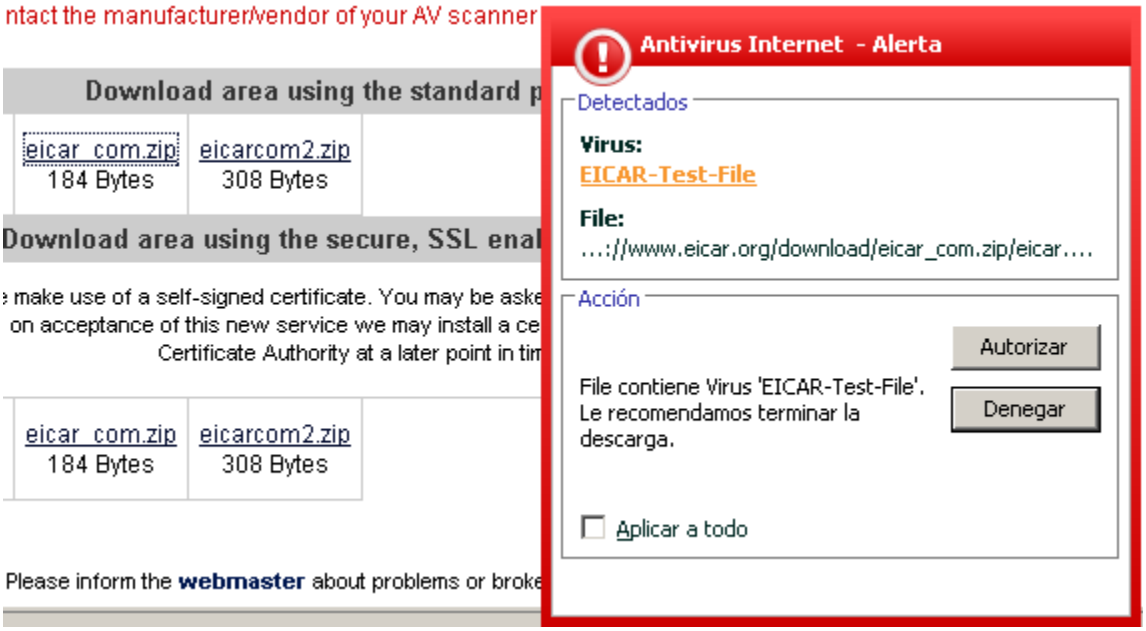

Figura 3. 17: Detección del fichero con código malicioso.

No se puede parar, no se puede renombrar, no se puede matar, no se puede borrar, etc. Su servicio está muy bien diseñado[ver figura 3.17 y 3.18]., mientras esté activo poco se puede hacer. La solución, como no podría ser otra, es que el servicio debe dejar de estar activo. [2]

Figura 3. 18: Alerta de sitio infectado.

Básicamente, la idea es inhabilitar el servicio. ¿El modo a prueba de fallos (safeboot) carga servicios adicionales como son antivirus? Sabemos que no. Por tanto, si se fuerza el arranque a prueba de fallos desde el boot.ini se elimina la protección del antivirus [ver figura 3.19].

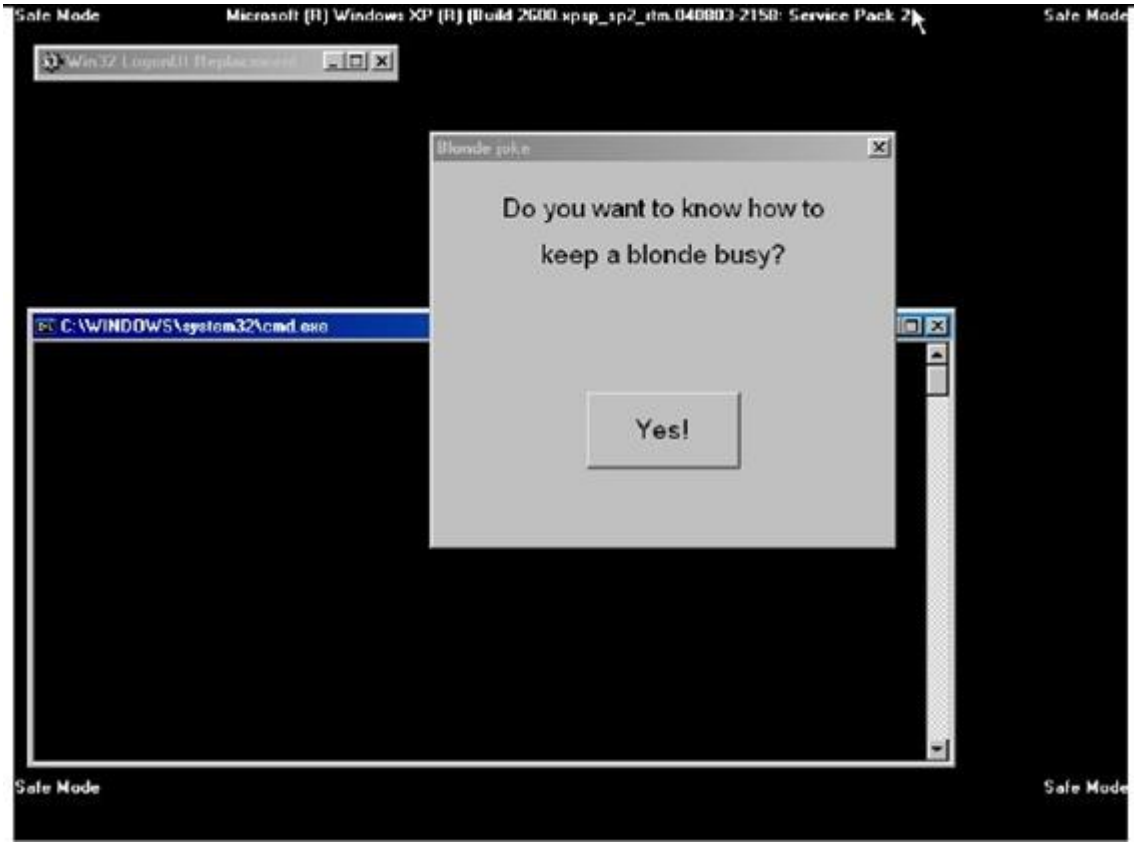

Figura 3. 19: Solo anulando el servicio.

3.9 Descifrado de Contraseñas.

Herramienta: Ophcrack. [20]

Prerrequisitos: Ninguno.

Contramedidas: Encriptación, políticas de fortalecimiento de contraseñas.

Descripción: Ophcrack es una herramienta para crackear las contraseñas de Windows basada en las tablas Rainbow [ver figura 3.20]. Es una implementación muy eficiente de estas tablas.

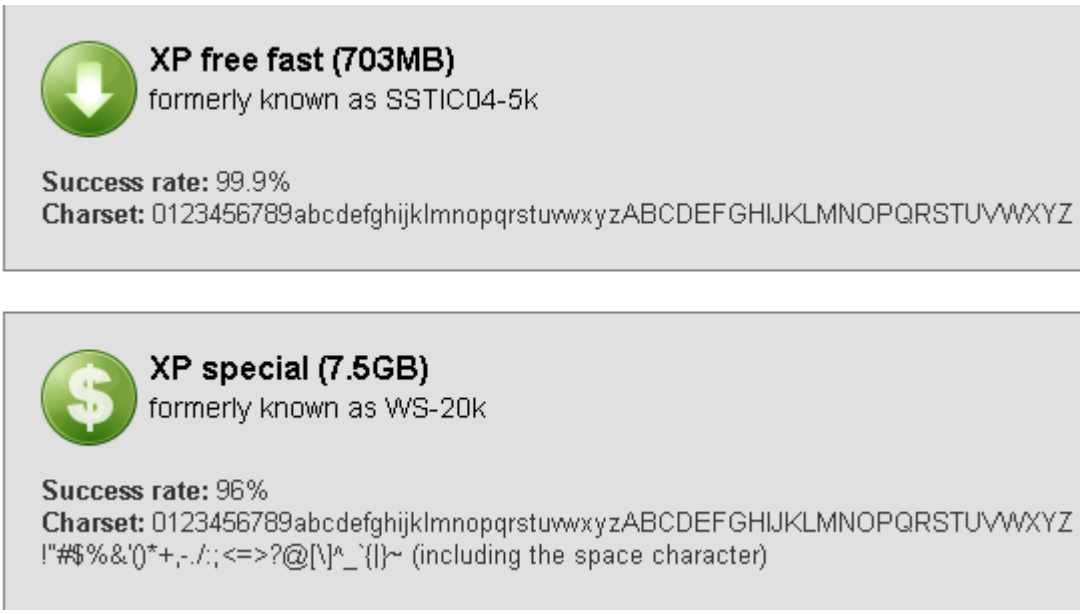

Figura 3. 20: Muestra de las combinaciones ofrecidas por las tablas.

Empezará el inicio del entorno gráfico. Después cargara el archivo SAM de nuestra partición Windows y empezará con la tarea de encontrar las contraseñas de las diferentes cuentas que existan.

Esto demorará dependiendo de la cantidad de caracteres usados en las contraseñas y de las posibilidades de nuestro PC [ver figura 3.21].

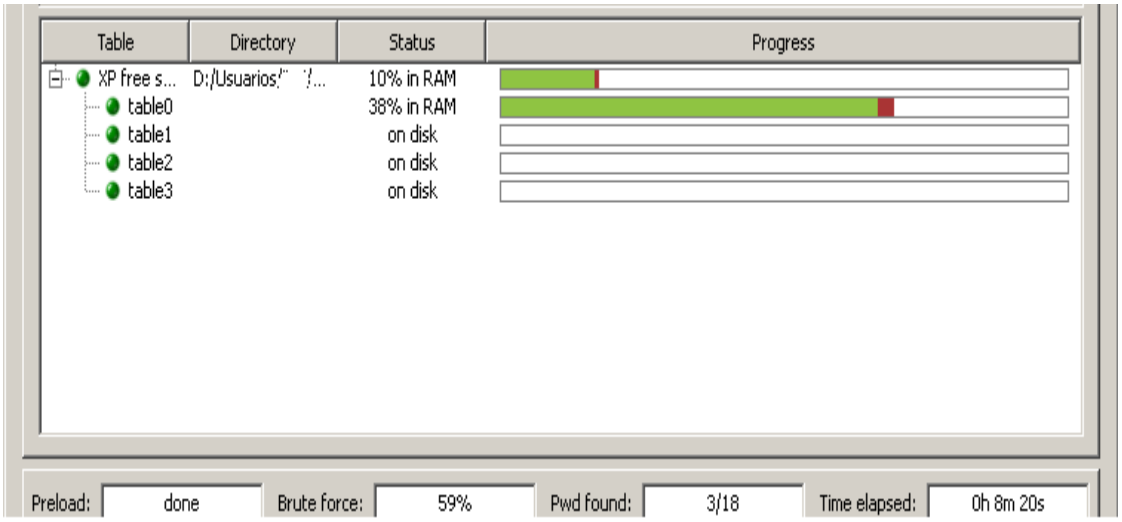

Figura 3. 21: Tiempo de Demorado en realizar la consulta.

El índice de éxito de acceso a claves es del 99,9%, para claves que contengan números y letras, sean todas mayúsculas o minúsculas. Es decir, la gran mayoría de claves poco seguras que cualquiera puede utilizar.

3.10 Elaboración de mapa de red.

Herramienta: LANsurveyor.

Prerrequisitos: Ninguno.

Contramedidas: Sistemas de detección de intrusos.

Descripción: Software para la gestión de redes e infraestructuras que monitoriza y salvaguarda las redes mediante diagramas automáticos de red, informes de gestión de activos, detección anti intrusiones. En este caso será usado para hacer mapas de red [ver figura 3.22].

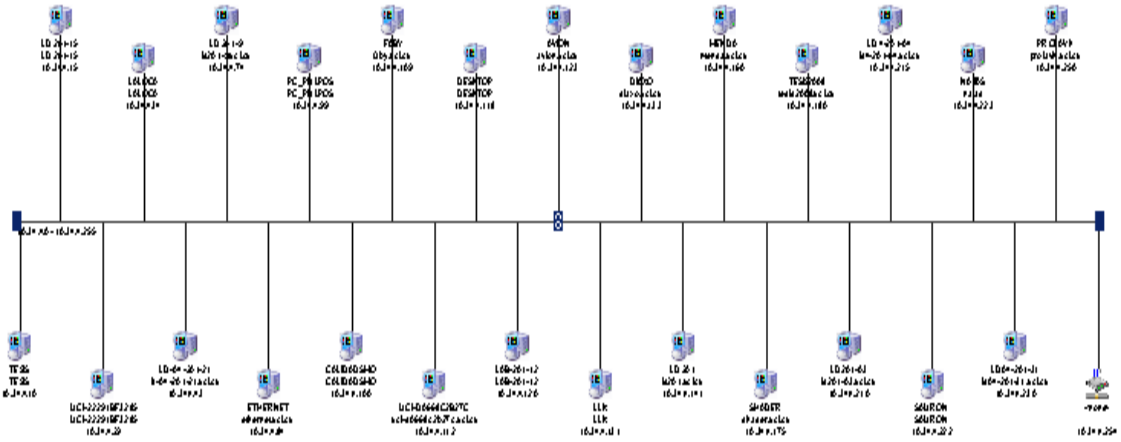

Figura 3. 22: Mapa de red.

3.11 Enumerar información de usuarios.

Herramienta: DUMPSEC. [6]

Prerrequisitos: Sesión nula.

Contramedidas: Restringir conexiones anónimas, Firewalls.

Descripción: La aplicación DUMPSEC esta diseñada para recolectar información de usuarios en la máquina objetivo, al igual que las herramientas anteriores hace uso de la API de Windows NetUserGetInfo, con la diferencia que esta ofrece una interfaz gráfica.
Procedimiento: Después de descargar e instalar, se ejecutar desde uno de los accesos creados por la instalación.

Ahora se va a **Report** y **select computer** y se ingresa la IP objetivo [ver figura 3.23].

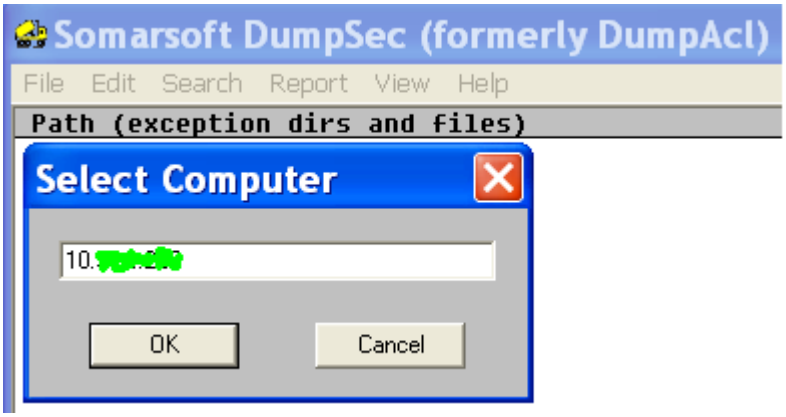

Figura 3. 23: Report y select computer.

Para los resultados de la enumeración le diremos que queremos ver el volcado por el usuario y como tabla [ver figura 3.24]. Seleccionamos todos los items. Clic en ok.

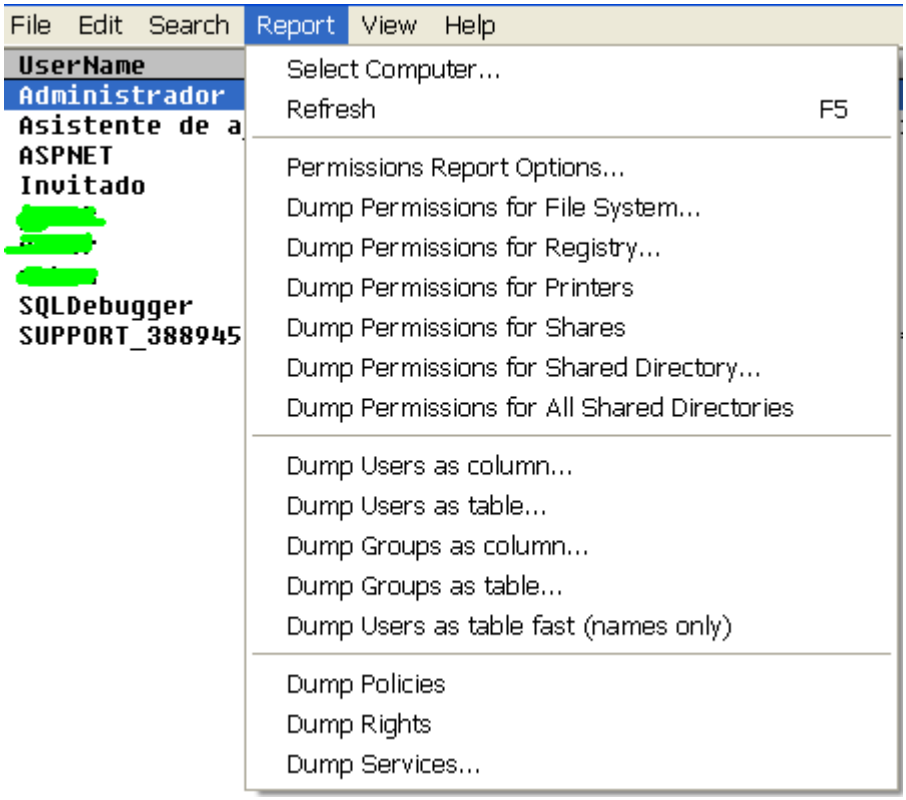

Figura 3. 24: Volcado del usuario.

A continuación se observaran los resultados ordenados como tabla. (Cada investigador puede analizar cada una de las formas de volcado de la herramienta). Rápidamente se observaran los usuarios de la máquina, grupos, comentarios, estado de la cuenta, último acceso, SID, caducidad de la contraseña, etc.

Además, la herramienta puede ser ejecutada mediante línea de comandos. Desde el directorio de instalación ejecutar la siguiente sintaxis:

dumpsec /computer=dirección IP /rpt=users /saveas=cvs /outfile=usuarios.txt

3.12 Resultados.

Luego de hacer uso de todo un conjunto de herramientas se hace necesario evaluar los resultados para examinar el estado en que se encuentra el sistema analizado. De esta forma se reúnen datos que: refuerzan el conjunto de políticas que domina la organización, ratifican las ya existentes o en algunos casos implante e implemente nuevas formas. Para esto nos referimos al documento que contenga las políticas de seguridad de la organización. A los efectos de esta tesis, se utilizara como apoyo las políticas de seguridad de la universidad.

1. Para el sistema operativo Windows XP las computadoras deben estar correctamente actualizadas con todos los parches de seguridad, se recomienda instalar Service Pack 3 que ya contiene la mayoría de las actualizaciones anteriores.
2. La contraseña empleada por los usuarios para acceder a sistemas locales tendrá una longitud de 15 caracteres como mínimo, y debe cumplir con varios requerimientos de complejidad como empleo de números, caracteres especiales, letras mayúsculas y minúsculas, para mayor dominio de la complejidad de la misma se recomienda visitar este vinculo en donde se prueba que tan elaborada puede ser la complejidad de una contraseña. [15]

   https://seguridad.uci.cu/index.php?option=com_content&task=section&id=18&Itemid=91

3. Mediante un estudio elaborar medidas para el fortalecimiento o prevención del robo del archivo de contraseñas (Sam) de la familia Windows, con aplicaciones del sistema tales como syskey e implementación de ntlmv2.
4. Verificar la existencia de una correcta secuencia de inicio en la BIOS así como que la misma esté protegida con contraseña.
5. Estudiar la posibilidad real de descompartir recursos del sistema tales como C$, ADMIN$, y en su defecto solo compartir lo necesario y con los privilegios administrativos que necesite.
6. Chequear las versiones y actualizaciones de los paquetes de programas instalados en las computadoras pues muchas versiones desactualizadas conllevan vulnerabilidades.
7. Velar por la constante actualización de los servidores de software.

8. Cuando se instalen aplicaciones o se brinden servicios que requieran un puerto de salida estándar y este sea configurable, analizar la opción de que no sea el definido por defecto. Esta recomendación viene dada por la facilidad de poder identificar un atacante el tipo de servicio o programa utilizado por el tipo de puerto que este abierto en una computadora.
9. Fortalecer la política de auditoria mejorando las formas de auditar los sucesos en la PC mediante la habilitación de las directivas correspondientes. Esto aumenta las posibilidades de poder analizar los pasos seguidos por un atacante una vez que vulnero un sistema. Para habilitar esta función se va a la ventana de Configuración de Seguridad Local\Directivas Locales\Directiva de auditoria\Auditar suceso de inicio de sesión [ver figura 3.25]

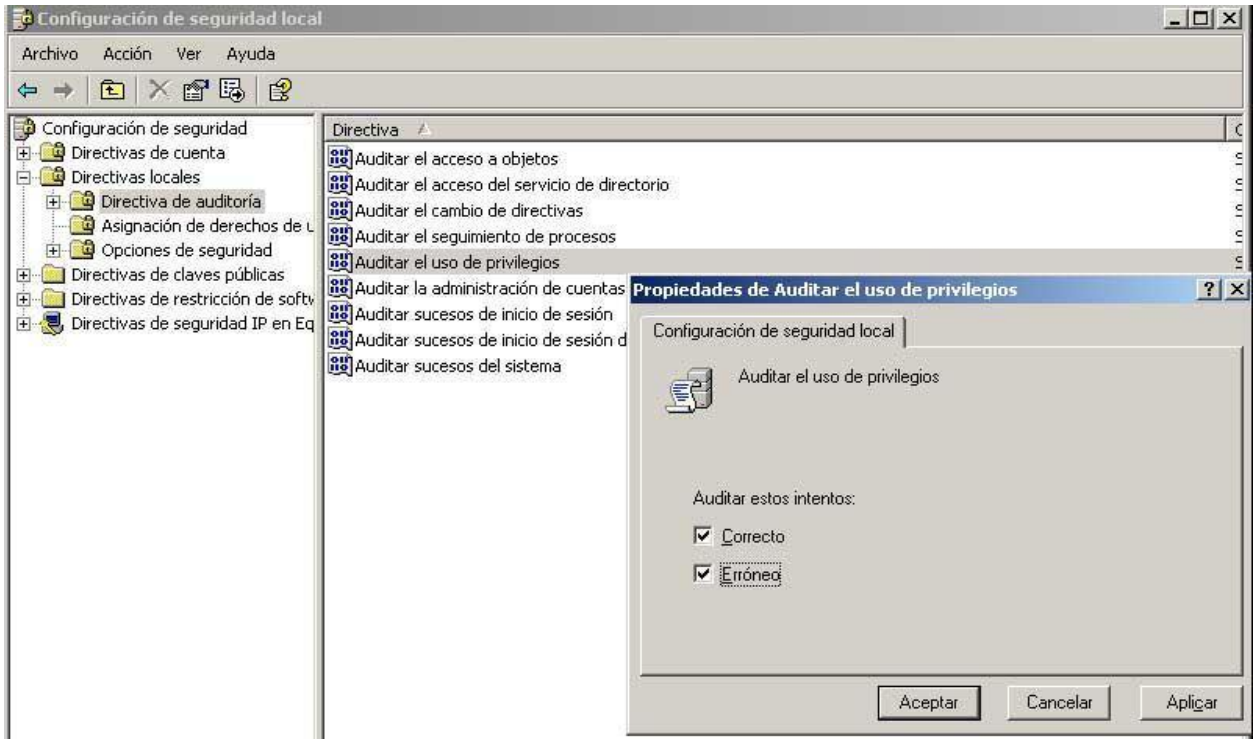

Figura 3. 25: Auditar suceso de inicio.

Local\Directivas Locales\Directiva de auditoria\Auditar acceso a objeto [ver figura 3.26] [20].

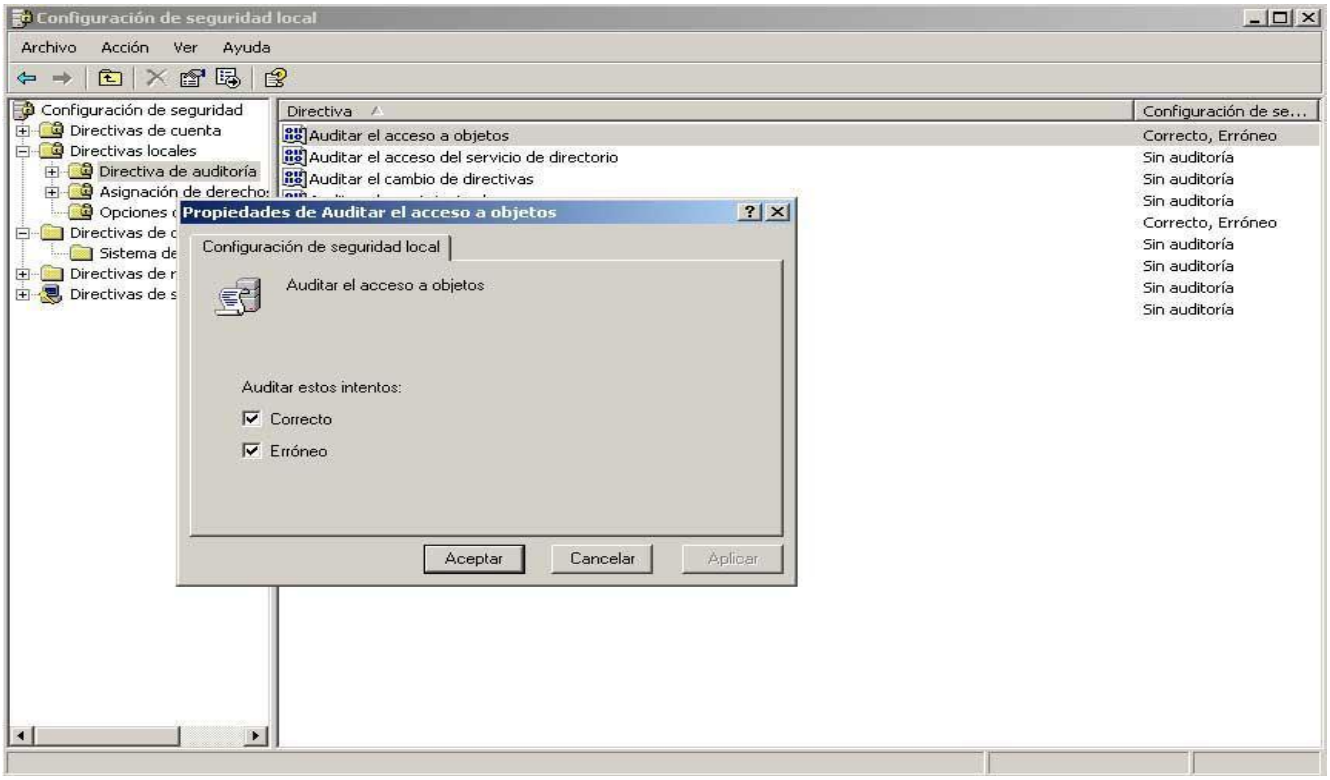

Figura 3. 26: Auditar acceso a objeto.

10. Evitar cualquier forma de recordar las contraseñas en el sistema.
11. Configurar el uso de sesiones nulas en los equipos para esto:
    - ❖ Inicie el Editor del Registro.
    - ❖ Busque y haga clic en la siguiente clave del Registro:
        - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
    - ❖ En el menú Edición, haga clic en Agregar valor y agregue el valor siguiente al Registro:
        - Nombre de valor: RestrictAnonymous.
        - Tipo de datos: REG_DWORD.
        - Valor: 2
        - Valor predeterminado: 0

- Un valor 2 restringe las conexiones de sesión nula. Para configurar el valor RestrictAnonymous, cambie la clave del Registro a 0 o a 1 para Windows NT 4.0, o a 0, 1 ó 2 en el caso de Windows 2000.
- Estos números corresponden a las configuraciones siguientes:
- 0 Ninguna. Se basa en los permisos predeterminados.
- 1 No permite la enumeración de nombres y cuentas de SAM.
- 1 No permite la enumeración de nombres y cuentas de SAM.

❖ Reinicie el equipo.

El beneficio que trae eliminar las sesiones nulas en los equipos consiste en no ofrecer determinada información vital que puede ser utilizada para realizar ataques en el sistema o incluso poder acceder a recursos no autorizados con este tipo de sesión.

Conclusiones.

En este capítulo se vio como se aplicó un grupo de herramientas en distintas partes de una red. También se vio reflejado como estos programas actúan generando un conjunto de datos útiles que permiten conocer en que estado de seguridad en que se encontraba ese entorno donde las herramientas fueron aplicadas. Estos datos se vuelven esencialmente útiles a la hora de plantearse como crear medidas que favorezcan la erradicación de este grupo de vulnerabilidades para así potenciar la minimización del riesgo de incidentes de seguridad. Esto favorece enormemente el entorno informático pues si minimizamos las vulnerabilidades se contribuye a eliminar las posibilidades de las que puede aprovecharse un usuario malintencionado. Como el mayor porcentaje de las estaciones de trabajo de centro están bajo sistemas de la familia Microsoft, el conjunto de pruebas responde a esta particularidad e incluso las recomendaciones dadas para la mejoría son enteramente aplicables en este entorno.

Conclusiones Generales

Para el cumplimiento de los objetivos y en concordancia con las exigencias hechas en el plan trazado, se realizó el estudio de los test de penetración más usados en la actualidad, para adaptarlos a las necesidades de nuestra organización, así como la ejecución de las tareas planteadas para el logro del proyecto. Además se hace una reseña general de la evolución de la seguridad informática, así como contenidos afines con el funcionamiento de esta rama y conceptos fundamentales. Destacar en el trabajo la descripción y propuesta de un grupo de herramientas aplicadas en distintos puntos de la red. También se vio reflejado como estos programas actúan generando un conjunto de datos útiles que permiten conocer el estado en que se encuentran los lugares donde las herramientas fueron aplicadas. Estos datos se vuelven esencialmente útiles a la hora de clasificar los riesgos que posee la organización en la que se apliquen el conjunto de pruebas y también favorece como plantearse medidas que ayuden a disminuir el grupo de vulnerabilidades detectadas, para así potenciar disminuir los riesgos de incidentes de seguridad. De las metodologías principales que se analizan se selecciona la OSSTMM ya que durante la investigación se puede comprobar que la mayoría de los test de penetración son basados en esta metodología dado la sencillez de la descripción de sus pasos, la facilidad de entendimiento que ofrece incluso a personas que no dominen tan profundo el tema de seguridad, por ser un documento en constante actualización y no ser superfluo. El entorno analizado esta constituido mayoritariamente por el sistema operativo de la familia Windows de Microsoft por lo que fue necesario orientar las pruebas hacia esta plataforma, aunque muchas de las herramientas presentan una contraparte en sistemas de código abierto, la totalidad de los test están desarrollan desde Windows eso no impide poder arrojar resultados de computadoras con sistemas operativos diferentes como de hecho los demuestran algunas pruebas realizadas. Se hace necesario señalar una de las dificultades principales del desarrollo de este trabajo de diploma fue la selección y búsqueda del conjunto de herramientas a utilizar ya el uso de este tipo de herramientas muchas veces esta limitado por considerarse armas de doble filo, pues en las manos equivocadas los datos generados por estas herramientas pueden ser utilizados para la realización de ataques sofisticados.

Recomendaciones

Se recomienda por su importancia implementar además test de penetración en las áreas siguientes:

- Bases de datos.
- Web.
- Redes inalámbricas.
- Seguridad en Internet.
- Seguridad física.
- Equipos interconectores.
- Se recomienda dar continuidad al estudio de los Test de penetración ya que este campo está en constate evolución y los métodos y medios para violar la seguridad informática son cada vez más novedosos y elaborados.
- Se recomienda la creación de un grupo especializado en la implementación de test de penetración en la universidad.
- Recomendarla elaboración de un test de penetración para sistemas Unix/Linux.

Referencia Bibliográfica

[1]. Lic. Siura Libertad Arregoitia López. 1998. http://www.fgr.cu. [En línea] 1998. [Citado el: 25 de Diciembre de 2007.] http://www.fgr.cu/Biblioteca%20Juridica/Derecho%20y%20Delitos%20Informaticos/LOS%20LLAMADOS%20DELITOS%20INFORMATICOS%20SU%20REGULACI%D3N%20PENAL%20EN%20CUBA.doc.

[2]. *Anulando la detección de ficheros.* **FraMe. 2007.** Murcia : s.n., 2007.

[3]. Borghello, Lic. Cristian. 2001. *Seguridad Informática - Implicancias e Implementación.* s.l. : http://www.segu-info.com.ar/tesis/, 2001.

[4]. Cano, J. "Concepto Extendido de la Mente Segura: Pensamiento Sistémico en Seguridad Informática". *http://www.alfa-redi.org.* [En línea] [Citado el: 12 de enero de 2008.] http://www.alfa-redi.org/rdi-articulo.shtml?x=3932.

[5]. Colectivo de autores. 2008. http://labs.dragonjar.org. [En línea] 13 de mayo de 2008. [Citado el: 29 de Junio de 2008.] http://labs.dragonjar.org/laboratorios-hacking-tecnicas-y-contramedidas-identificacion-de-banner%E2%80%99s-banderas-part-i.

[6]. 2008. http://labs.dragonjar.org. [En línea] 13 de Mayo de 2008. [Citado el: 28 de Junio de 2008.] http://labs.dragonjar.org/laboratorios-hacking-tecnicas-y-contramedidas-enumeracion-del-objetivo-i.

[7]. 2008. http://www.dragonjar.org. [En línea] 13 de Mayo de 2008. [Citado el: 27 de Junio de 2008.] http://www.dragonjar.org/laboratorio-hacking-tecnicas-y-contramedidas-scanning-i.xhtml.

[8]. 2008. http://www.dragonjar.org. [En línea] 13 de Mayo de 2008. [Citado el: 25 de Junio de 2008.] http://www.dragonjar.org/laboratorio-hacking-tecnicas-y-contramedidas-sniffing.xhtml.

[9]. 1997 / 2008. http://www.scd.com.ar. [En línea] SCD Servicios Informáticos S.R.L., 1997 / 2008. [Citado el: 18 de Febrero de 2008.]

[10]. http://www.scd.com.ar/servicios_corporativos/que_comprende_la_auditoria_de_seguridad.html.

[11]. ISO/IEC 17799. [En línea] [Citado el: 27 de junio de 2008.]

[12]. http://es.wikipedia.org/wiki/ISO/IEC_17799.

[13]. Colectivo de autores. http://www.informaticajuridica.com. [En línea] [Citado el: 17 de Enero de 2008.] http://www.informaticajuridica.com/trabajos/Proteccion_contra_los_delitos_informaticos_en_Cuba.asp.

[14]. http://www.oissg.org. [En línea] [Citado el: 12 de Febrero de 2008.] http://www.oissg.org/content/view/71/71/.

[15]. Colectivo de trabajadores. 2006. *Políticas de Seguridad Informática de la UCI. Dirección de Redes y Seguridad Informática.* 2006.

[16]. Cordoves, Enrique. 2006. http://www.alfa-redi.org. [En línea] SEptiembre de 2006. [Citado el: 20 de Enero. de 2008.] http://www.alfa-redi.org/rdi-articulo.shtml?x=7178. No. 098.

[17]. Deloitte Touche. 2008. *Test de intrusión.* Barcelona : s.n., 2008.

[18]. Enrique Cordoves. 2006. http://www.alfa-redi.org. [En línea] Agosto de 2006. [Citado el: 25 de Enero de 2008.] http://www.alfa-redi.org/rdi-articulo.shtml?x=6958. No. 097.

[19]. 2007. http://elladodelmal.blogspot.com. [En línea] 27 de Febrero de 2007. [Citado el: 26 de Junio de 2008.] http://elladodelmal.blogspot.com/2007/02/test-de-intrusion-i-de-vi.html.

[20]. *Olfateando contraseñas en sistemas Microsoft.* **DDiego. 2008.** 2008.

[21]. Pete Herzog. 2003. *OSSTMM 2.1.Manual de la Metodología Abierta de Testeo de Seguridad.* 2003.

[22]. Websense Security Labs. 2008. http://www.WebsenseSecurityLabs.com. [En línea] 2008. [Citado el: 20 de Diciembre de 2007.] www.websense.com/securitylabs/docs/2008_Threat_Predictions_ES.pdf.

Índice de figuras.

Glosario de Abreviaturas

UCI: Universidad de las Ciencias Informáticas

AC: Antes de Cristo.

ACM: Association Computery Machine.

IEEE: Institute of Electric and Electronic Engineers.

EDPAC: Electronic Data Processing Association.

ISACA: Information System Audit and Control Association.

DoD: Departamento de Defensa de los Estados Unido.

VPN: Virtual Private Networks, en castellano red privada virtual.

MAC: Ministerio de Auditoria y Control.

No: Número.

DTI: Departamento técnico investigativo.

IP: El terminó informático de protocolo de internet.

LAN: Designa a una red de área local, conocida por sus siglas en inglés LAN.

OSSTMM: Open Source Security Testing Methodology Manual.

ISSAF: Information Systems Security Assessment Framework.

OISSG: Open Information Systems Security Group.

IT: Information Technologies, Tecnologías de la Información.

ISO: Organización Internacional para la Estandarización.

ISP: (Internet Service Provider) Proveedor de servicios de Internet.

ASP: Acrónimo de Application Service Provider (Proveedor de Servicios de Aplicaciones). Las ASP, también denominadas netsourcing, son empresas que alquilan aplicaciones informáticas a sus clientes a través de Internet.

TCP: Transmission Control Protocol, es uno de los protocolos de comunicaciones sobre los que se basa Internet.

UDP: Acrónimo de User Datagram Protocol (Protocolo de datagrama a nivel de usuario), perteneciente a la familia de protocolos TCP/IP.

ICMP: Internet Control Message Protocol. Protocolo de la capa IP para la generación de mensajes de error.

ACL: Access Control Lists o Lista de Control de Acceso.

DMZ: (Demilitarized zone) Es una opción de los routers o switch, en donde se re direccionan automáticamente los puertos a las estaciones conectadas a una ip. Se utiliza normalmente para servidores web, ftp, mail, etc.

NAT: Network Address Translation. Es un estándar de Internet que le permite a una red local LAN usar un grupo de direcciones de IP.

TTL: Time To Live.Tiempo de Vida. Contador interno que incorporan los paquetes.

WLAN: WLAN (inglés < Wireless Local Area Network) es un sistema de comunicación de datos inalámbrico.

Ghz: El hercio, hertzio o hertz es la unidad de frecuencia del Sistema Internacional de Unidades. Proviene del apellido del físico alemán Heinrich Rudolf Hertz, quien descubrió la propagación de las ondas electromagnéticas. Su símbolo es Hz (escrito sin punto como todo símbolo).El Gigahertz (GHz) es un múltiplo de la unidad de medida de frecuencia (hertz) y equivale a 109 Hz.

MBps: Megabit por segundo. Es una unidad que se usa para cuantificar la velocidad de transmisión de información equivalente a 1000 kilobits por segundo o 1000000 bits por segundo.

SSID: Service Set Identifier.

XSS: Es el ataque basado en la explotación de vulnerabilidades del sistema de validación de HTML incrustado.

SQL: Lenguaje de Consulta Estructurado (Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales.

HTML: El HTML, acrónimo inglés de HyperText Markup Language (lenguaje de marcas hipertextuales).

LDAP: LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado.

URL: Acrónimo de Universal Resource Locator (Localizador Universal de Recursos /Identificador Universal de Recursos). Sistema unificado de identificación de recursos en la red.
Es el modo estándar de proporcionar la dirección de cualquier recurso en Internet.

Unix: Sistema operativo multitarea y multiusuario. Existen distintas versiones realizadas por distintas casas, como AIX, XENIX, SCO, Linux, etc.

SMB: Sigla de Server Message Block (Bloque de mensajes de servidor), SMB es el protocolo de comunicación que usan los sistemas operativos.

NT: Sistema Operativo orientado a servidor de Microsoft, basado en su interfaz gráfico

Windows.

PDF: (Portable Document Format o Formato de Documento Portátil) Formato de documentos de Adobe.

Dos: Denegación de Servicios.

DDoS: Un ataque DDOS (Distributed Denial Of Service Attack) o Ataque de Denegación de Servicio Distribuido es un tipo especial de DoS.

SMTP: (Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo).

POP3: Protocolo estándar utilizado para recuperar correo electrónico almacenado en un servidor de correo.

HTTP: Protocolo de Transmisión Hipertexto. Protocolo de comunicaciones utilizado por los programas clientes y servidores de WWW para comunicarse entre sí.

HTTPS: El protocolo HTTPS es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL).

FTP: file transfer protocol. Véase protocolo de transferencia de archivos.

AVS: Antivirus.

IDS: Sistema de detección de intrusos.

PBX: Centralita (también denominada Central Telefónica para Negocios Privados) – es una central telefónica propiedad de una empresa privada, en contraposición con la central que es propiedad de un operador de telecomunicaciones o de una empresa de telefonía.

SSH: Protocolo de conexión segura a los servidores. Igual que Telnet pero los datos se envían y reciben encriptados.

IPSEC: IP Security. Es un conjunto de protocolos desarrollados por la IETF para dar soporte al intercambio seguro de paquetes del lado del IP. El IPsec se implementó ampliamente en las Redes Privadas Virtuales (VPNs). Soporta dos modos de encripción: Transport y Tunnel.

MAC: Media Access Control address .Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.

ODBC: ODBC son las siglas de Open DataBase Connectivity, que es un estándar de acceso a Bases de Datos desarrollado por Microsoft Corporation.

ECHO: echo es un comando para impresión en pantalla, utilizado en las terminales de los sistemas operativos por ejemplo Unix, GNU/Linux, MS-DOS; dentro de pequeños programas llamados scripts. Existen lenguajes de programación tales como PHP que también lo utilizan con el mismo fin.

DNS: Servidor de nombres de dominio (Domain Name Server).

SAM: El archivo SAM, conocido más comúnmente como "la SAM" es el archivo de Log en el que se encuentran los datos y las contraseñas de todas las sesiones de un ordenador que incorpore un sistema operativo Windows.

SO: Sistema operativo.

PC: Ordenador personal o Computadora Personal - Personal Computer en inglés.

Glosario de Términos

Acceso Remoto: Se define como un acceso desde el exterior de la ubicación.

Acuerdo de No Divulgación: Acuerdo legal que evita la difusión de información mas allá de los propósitos informativos, entre las partes que mantienen dicho acuerdo de no divulgación.

Ámbito de la Red: Se refiere a lo que el testeador puede legalmente testear.

Auditoria de Seguridad: Inspección manual con privilegios de acceso del sistema operativo y de los programas de aplicación de un sistema. En los Estados Unidos y Canadá,

Auditor: representa un vocablo y una profesión oficiales, solamente utilizado por profesionales autorizados. Sin embargo, en otros países, una "auditoria de seguridad" es un término de uso corriente que hace referencia a Test de Intrusión o test de seguridad.

Caja Blanca: El testeador posee conocimiento previo integral de los elementos o del entorno a ser testeados.

Caja Gris: El testeador tiene un conocimiento previo de los elementos o del entorno a testear.

Caja Negra: El testeador no tiene conocimiento previo de los elementos o del entorno a testear.

Cliente: Se refiere al receptor de las ventas con quien se la confidencialidad esta éticamente implícita sin firmarse un acuerdo de no divulgación o contrato alguno.

Cortafuegos: Las herramientas de software o hardware que impone una Lista de Control de Acceso en un sistema o red.

Hacker: Una persona inteligente que tiene una curiosidad natural, le gusta aprender como las cosas funcionan, y le interesa conocer técnicas de evasión o abusar de procesos para ver qué sucede.

Hacking Ético: Una forma de test de intrusión originalmente usado como táctica de mercadeo, que

significa un test de intrusión en todos los sistemas - y donde hay más de un objetivo, generalmente todo es un objetivo.

Seguridad Práctica: Define la seguridad que puede ser empleada y que se aplica a la justificación de negocios.

Sistemas de Detección de Intrusiones (IDS): Ya sean activos o pasivos, basados en terminales o en la red, esta herramienta está diseñada para monitorear y a menudo detener ataques cuando suceden.

Sombrero Blanco: Es un hacker que no transgrede la ley y actúa con ética.

Sombrero Gris: Un hacker que es caótico, anarquista, pero no infringe la ley. Sin embargo, sus acciones a menudo carecen de integridad o ética.

Sombrero Negro: Un hacker que es caótico, anarquista e infringe la ley.

Test de Intrusión: Test de seguridad con un objetivo definido que finaliza cuando el objetivo es alcanzado o el tiempo ha terminado.

Testeo Automatizado: Cualquier clase de testeo automatizado que también brinda análisis.

Testeo con Privilegios: Test donde las credenciales necesarias son suministradas al usuario y los permisos concedidos para testear con dichas credenciales.

Testeo de Verificación: Un test de verificación realizado en una segunda etapa luego de que todos los parches han sido aplicados.

Testeo de Vulnerabilidades: Test de servicios, puertos abiertos y vulnerabilidades conocidas.

Vishing: Es una práctica criminal fraudulenta en donde se hace uso del Protocolo Voz sobre IP (VoIP) y la ingeniería social para engañar.