ASEGURAMIENTO DE LOS SISTEMAS COMPUTACIONALES DE LA EMPRESA SITIOSDIMA.NET

ING. JAVIER HUMBERTO ROBAYO LÓPEZ
ING. RICHAR MAURICIO RODRÍGUEZ RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C. – ZIPAQUIRÁ
2015

SEGURAMIENTO DE LOS SISTEMAS COMPUTACIONALES DE LA EMPRESA SITIOSDIMA.NET

ING. JAVIER HUMBERTO ROBAYO LÓPEZ
ING. RICHAR MAURICIO RODRÍGUEZ RODRÍGUEZ

MONOGRAFÍA – ***Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net. Beneficios y riesgos de su implementación o no en cualquier organización.***

DIRECTOR
RAFAEL PÉREZ HOLGUÍN
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C. – ZIPAQUIRÁ
2015

PÁGINA DE ACEPTACIÓN

Nota de Aceptación

_____

_____

_____

Firma de presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

_____

DEDICATORIA

Dedicamos esta tesis en primera instancia a DIOS y nuestras familias de las cuales el apoyo y confianza ha sido parte fundamental para el desarrollo de nuestro proceso de formación académica.

A la Universidad Nacional Abierta y a Distancia la cual ha permitido que nuestro crecimiento profesional se fortalezca y nos genere mejores oportunidades en diferentes ambientes laborales.

A nuestros Maestros, compañeros y amigos que nos apoyaron y motivaron para lograr los objetivos que nos propusimos en el momento de tomar este reto como parte de nuestras vidas.

Al Ing. Rafael P. Holguín, quien como director ha sido timón y motivador para lograr hacer de éste proyecto una realidad.

CONTENIDO

LISTA DE FIGURAS

pág.

GLOSARIO

AMENAZA: es un hecho, incidente o persona que puede generar daños a un sistema informático, donde puede causar pérdida de información, destrucción de información o problemas funcionales de un sistema o red informática.

ANTIVIRUS: es un software diseñado para la detección de software con código malicioso o destructivo.

BOTNET: es una red de equipos donde se controlan desde un servidor el cual puede ejecutar instrucciones a los equipos infectados y realizar tareas de forma masiva.

CABALLO DE TROYA: es un código malicioso donde se logra integrar en un software legitimo otro con intensiones mal intencionadas, regularmente se activa el software legitimo e instantáneamente el software malicioso.

EXPLOITS O PROGRAMAS INTRUSOS: son códigos diseñados para aprovechar vulnerabilidades de sistemas operativos, programas o aplicaciones con debilidades en su estructura de desarrollo.

FIREWALL: es un software que identifica y bloquea intentos de intrusión a una red informática.

GUSANOS: es un código malicioso que logra auto propagarse por medio de vulnerabilidades o procedimientos no consientes de los usuarios.

INGENIERÍA SOCIAL: es un método de engaño donde se motiva al usuario a dar información personal como datos privados o contraseñas de acceso a sistemas de información.

KEYSTROKE LOGGER O PROGRAMA DE CAPTURA DE TECLADO (KEYLOGGER): es un código que al ser instalado en un computador captura las pulsaciones del teclado y los registra en un archivo de texto o los envía a un correo electrónico o servidor ftp.

PHARMING: es la alteración de los archivos HOST donde se puede redirigir el tráfico de un dominio a una IP determinada y capturar datos personales o instalar software malicioso.

PHISHING: técnica de captura de información por medio de páginas web falsas.

SPYWARE: software diseñado específicamente para el robo de información, se activa por medio del uso de programas o vulnerabilidades de los sistemas operativos.

RESUMEN

La seguridad de un sistema informático, empieza en la elección del sistema operativo y las características implementadas en su instalación. El Hardening, es un método que permite implementar tantas estrategias como herramientas en busca de un sistema operativo más seguro. En el presente trabajo, se da a conocer en detalle, qué es hardening, las actividades técnicas que se deberían tener en cuenta en su implementación, las configuraciones seguras y otras medidas aplicables.

Seguidamente, se analizan algunas herramientas relacionadas en el uso de una estrategia se seguridad Hardening. Tras la instalación de un sistema operativo quedan puertos abiertos por defecto, se verá de qué manera considerar cuáles deben mantenerse abiertos y cuáles deben cerrarse. De igual modo, se estudian aplicaciones que permiten monitorear el flujo de información entrante y saliente del sistema operativo y, de qué forma hacer que el Firewall sea más eficaz.

Igualmente se analiza, qué es un virus informático y sus métodos de infección, así mismo se estudian las principales funciones de un Antivirus y la clasificación de éstos. La implementación de IDS, Sistemas de Contraseñas seguras, criptografía, sniffers y adecuadas políticas de seguridad, hacen parte de un método integral de seguridad informática Hardening, temas aquí tratados.

Al concluir el estudio de las diferentes aplicaciones a implementar en hardening, se plantea *el aseguramiento de los sistemas operativos de la empresa sitiosdima.net*. Como Anexo, se presenta en ejemplo de Auditoría del Sistema.

Palabras Claves

CONFIGURACIÓN, ESTRATEGIA, HARDENING, HERRAMIENTAS, INFORMÁTICA, INSTALACIÓN, MÉTODOS, MONITOREAR, SEGURIDAD, SISTEMA OPERATIVO.

ABSTRACT

The security of a computer system, begins in the choice of operating system and the features implemented in your facility. The hardening is a method to implement many strategies as tools for a more secure operating system. In this paper, it's disclosed in detail, what's hardening, the technical activities that should be taken into account in its implementation, secure configurations and other measures applicable.

Afterward, some tools related to the use of a safety strategy Hardening is analyzed. After installing an operating system default ports are open, how will consider what should be kept open and which should close. Similarly, applications that allow you to monitor the incoming and outgoing operating system information and how to make more effective Firewall studied.

Also discussed, what a computer virus infection and its methods, also the main functions of an Antivirus and classification of these are studied. The implementation of IDS Systems Strong passwords, encryption, sniffers and appropriate security policies are part of a comprehensive approach to security hardening, topics make a speech. At the conclusion of the study of different applications to implement hardening, securing Operating Systems Sitiosdima.net Company arises. As Annex presents an example of System Audit.

Key Words.

HARDENING, INFORMATION, INSTALLATION, METHODS, MONITORING, OPERATING SYSTEM, SECURITY, SETTING, STRATEGY, TOOLS.

1. INTRODUCCIÓN

Actualmente las empresas ingresan a las nuevas tecnologías de la información, iniciando nuevos desafíos frente a procesos enmarcados en la seguridad informática y la seguridad de la información, siendo estas un objetivo más de ataques informáticos tanto externos como internos. El *Aseguramiento de los sistemas computacionales de la empresa Sitiosdima.net* se presenta como la opción sobre la cual se realizarán pruebas que permitirán constatar hipótesis respecto al nivel de seguridad antes y después de implementar diferentes métodos de Hardening (Endurecimiento) en un sistema computacional.

Así, los sistemas de información, redes de datos, sistemas operativos y la manipulación no apropiada de la información por parte de los usuarios, han hecho que cada día se presenten más opciones para los delincuentes informáticos, por ello el aseguramiento en profundidad de los sistemas operativos toman una importancia vital para ser proactivos frente a posibles intrusiones, esto con el fin de limitar en lo posible vulnerabilidades y evitar perdida de información o manipulación de los equipos comprometidos. Por lo anterior es evidente que surge la necesidad de aplicar las técnicas de aseguramiento Hardening en los sistemas operativos de las empresas, con ello se minimizan riesgos y se evitan consecuencias económicas, afectación de imagen entre otras consecuencias.

Como se verá a lo largo del desarrollo de ésta monografía, asegurar un sistema requiere muchas veces desactivar servicios, limitar características de software y bloquear otras tantas que pueden ser fácilmente la puerta de entrada al sistema, de ésta manera se está reduciendo en importante medida un gran número de vulnerabilidades. Cada organización tiene sus propias necesidades, en el desarrollo de ésta investigación se pretende dar a conocer de manera unificada las características de las diferentes aplicaciones que se convierten en herramientas

fundamentales y de uso imperativo en el hardening de los sistemas informáticos (Firewall, Antivirus, IDS, Criptografía, usos de Sniffer, entre otros). De esta manera, inicialmente se estará dando nociones básicas de qué es y en qué consiste el Hardening, así como su implementación.

Seguidamente se estará tabulando información recabada de la Web respecto a las distintas aplicaciones de Software y sus características básicas que se utilizan en todo el proceso de aseguramiento de los sistemas operativos, se quiere con esto poner en conocimiento de empresarios y demás personal inmerso y comprometido con la seguridad informática que existen grandes posibilidades tanto como herramientas que brindan muchas opciones para ser usadas estratégicamente reflejándose en niveles importantes de confiabilidad y reducción de vulnerabilidades.

Para que cualquier proceso de aseguramiento sea exitoso, debe ser complementado con políticas de seguridad de alta exigencia que a su vez requiere de adecuada capacitación tanto a administradores del sistema, como a los usuarios. Aun así, se entiende que no hay sistema totalmente inmune a cualquier vulnerabilidad, hay conocimiento que implementar éste proceso es un paso muy importante en pro de la seguridad informática de cualquier organización.

2. TÍTULO

ASEGURAMIENTO DE LOS SISTEMAS COMPUTACIONALES DE LA EMPRESA SITIOSDIMA.NET

3. DEFINICIÓN DEL PROBLEMA

Hasta qué punto se tiene conocimiento de las aplicaciones empleadas en Hardening y estrategias de seguridad informática. En el desarrollo de la presente monografía se espera dar claridad respecto a qué tipo de software se está implementando para tal caso, sus características principales junto con sus beneficios de uso.

Hoy en día son incontables las diferentes aplicaciones que se pueden utilizar para aplicar diferentes métodos de Hardening en sistemas informáticos, pero muy poco se conoce de los elementos que lo componen, características y servicios que brindan. Por ende se planeó la realización de ésta monografía en la cual se espera plasmar los diferentes datos encontrados y de ésta manera contribuir a despejar inquietudes al respecto en la comunidad interesada en el tema.

Implementar las herramientas en estrategias de hardening, requiere conocer en detalle sus características ya que de ésta manera se puede aplicar al máximo todas las bondades de la aplicación que se quiere emplear según las necesidades de cada organización. Por ende*, el aseguramiento de los sistemas computacionales de la empresa sitiosdima.net* se usará como escenario de prueba e implementación de las diferentes herramientas aquí señaladas tras la investigación y puesta en conocimiento de su aplicabilidad según el caso.

Es claro que así como la empresa sitiosdima.net o cualquier otra organización deben contar con un proceso de hardening basado en el concepto de “defensa en profundidad”[1], fomentando actividades que permitirán minimizar riegos de fuga de información, vulneración de los sistemas operativos y la pérdida económica o de

[1] PARSON, Lexers. Modelo de seguridad en Profundidad. {En línea}. {21 de Junio de 2015}. Disponible en: (http://www.guatewares.com/2014/04/modelo-de-seguridad-en-profundidad.html).

información digital que ponga en riesgo la continuidad del negocio. Por ello, la realización de un proceso de Hardening exitoso, solo será posible si se tiene un conocimiento adecuado de las fortalezas y debilidades que puede brindar cada una de las distintas Aplicaciones de Software que se implementan en cada una de las estrategias y métodos acorde a los requerimientos de cada organización.

3.1 ACTIVIDADES PROPIAS DE UN PROCESO DE HARDENING

Castro[2] señala el hardening en términos primarios como un "endurecimiento", tal y como lo refleja su traducción del inglés. Dentro de las actividades, distingue las siguientes:

- "Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina"[3]. El autor señala dentro de estas algunas como el Upgrade de firmware, la complejización de contraseñas complejas en el arranque del equipo, así como "la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de dispositivos ópticos, USB o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo"[4].

- Instalación segura del sistema operativo. Para tal fin, Castro sugiere la consideración de al menos particiones primarias. Una primera para el

[2] CASTRO, Paul. Blog.smartekh. {En línea}. {8 de Febrero de 2015}. Disponible en: (http://blog.smartekh.com/%C2%BFque-es-hardening/).

[3] Ibídem.

[4] Ibídem.

sistema operativo en sí y otra para carpetas y archivos de importancia. También plantea el empleo de sistema de archivos "que tenga prestaciones de seguridad, y el concepto de instalación mínima, es decir, evitando la instalación de cualquier componente de sistema que no sea necesario para el funcionamiento del sistema"[5].

- Activación y/o configuración adecuada de servicios de actualizaciones automáticas. En este sentido se espera proveer de manera actualizada todos los parches de seguridad. Menciona el autor ´la posibilidad de instalar un servidor automático de actualizaciones que debe previamente una prueba en "un entorno de laboratorio el impacto de la instalación de actualizaciones antes de instalarlas en producción"[6].

- La última actividad destacada por Castro es la de la "instalación, configuración y mantención de programas de seguridad tales como Antivirus, Antispyware, y un filtro Anti spam"[7], de acuerdo con los requerimientos del entorno.

Estas tareas pueden concretarse dentro de una línea extensa de tiempo y abarcar varias subactividades. La tarea, según Castro es en líneas generales robustecer el equipo de tal forma que quede lo más posiblemente restringido. Sin embargo, anota el autor, todas estas medidas pueden terminar pasándole cuenta de cobro al usuario y convertirse más en una molestia que en una ayuda. En este sentido, Castro anota las tensiones entre la seguridad y versatilidad.

> "A medida que se busca una seguridad mayor en los sistemas, la versatilidad y facilidad de uso del mismo se ven limitados, puesto que

[5] Ibídem.
[6] Ibídem.
[7] Ibídem.

> la cantidad de decisiones que puede tomar el usuario se reduce y la cantidad de posibilidades ajenas al propósito inicial del sistema en sí disminuye drásticamente”[8].

Castro anota la paradoja e incompatibilidad que representa el aumentar la versatilidad y la facilidad de uso de los sistemas, anotando que con esto se ejerce presión con el aumento en las decisiones y posibilidades del usuario. “Lo que por consiguiente aumenta la probabilidad del mismo de equivocarse y poner en peligro la seguridad de todo el sistema. Y el debate sobre el punto exacto de equilibrio en cuanto a la cantidad de decisiones que deben pasar por manos del usuario final es bastante extenso y no está del todo resuelto”[9].

Finalmente, la cuestión es si el hardering es una ayuda y hasta qué punto puede afectar la concreción del objetivo inicial del sistema. Una respuesta difícil de encontrar, pero que bien puede ser orientada por la siguiente apreciación de Gutiérrez del Moral[10]

“Si un sistema trabaja con impresoras, redes inalámbricas y además con correo electrónico, no es recomendable deshabilitar la cola de impresión, el servicio de redes inalámbricas ni bloquear los puertos de SMTP y POP. En otras palabras, en cada acción de Hardening que se vaya a ejecutar en el sistema operativo, hay que tener especial cuidado en que dichas acciones no afecten el propósito del sistema en sí.”[11]

[8] Ibídem.

[9] Ibídem.

[10] GUTIÉRREZ DEL MORAL, Leonardo. 2013. Curso de Ciberseguridad y Hacking Ético. Editorial Punto Rojo Lbros. Sevilla, España. Disponible en: http://bit.ly/1W2gMOw

[11] Ibídem, p. 560

4. JUSTIFICACIÓN

Las organizaciones vienen siendo objeto de incontables intentos a diario por hacerse a la información y control de sus equipos de cómputo por parte de los delincuentes informáticos. Para muchas de las empresas que han sido víctimas de ataques informáticos, no ha sido prioridad capacitar el personal y la indagación respecto a las posibles medidas de seguridad que deben tomarse para prevenirlos.

Por ende, el desarrollo de la presente monografía (Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net) se convierte en una necesidad de gran importancia la cual pretende indagar y poner en conocimiento de empresarios y usuarios las diferentes herramientas que se encuentran disponibles en pro de elevar el nivel de seguridad informática de la organización.

Al tener conocimiento de las características de las aplicaciones que se vienen implementando en materia de seguridad informática, es más probable acertar en el diseño estratégico del plan de seguridad que requiere determinada empresa. Este trabajo será indudablemente material de consulta que dará nociones importantes en el diseño e implementación de Hardening (robustecimiento) de manera acertada para cualquier organización previniendo gran cantidad de riesgos a los cuales se están expuestas.

Según Sánchez[12]:

> "Cada entrada tiene un origen en común: cumplir los objetivos del negocio; deben basarse en una política de seguridad institucional e incluso tener un tratamiento diferente y ejecutarse en tiempos distintos ¿A qué me refiero con

[12] SÁNCHEZ, Eduardo Patricio. {En línea}. {14 de Enero de 2015}. Hardening. Disponible en: (http://www.magazcitum.com.mx/ ?p=2109#.ViUM_n4veM8)

> esto?, antes de salir a producción, cualquier sistema debería pasar por un proceso de fortalecimiento que le permita cumplir con la líneas base de seguridad establecida de acuerdo a su tipo. Tiempo después es fundamental que la organización mida si esta línea base de seguridad sigue cumpliendo con su objetivo primordial y para ello puede ejecutar estudios de análisis de vulnerabilidades, los cuales alimentan tanto el proceso de remediación como el proceso de fortalecimiento y la actualización de la línea base de seguridad."[13]

El autor así expresa la necesidad de que toda compañía blinde sus sistemas, y establece que deben cumplir al menos los estándares mínimos satisfactorios. Según el autor, el análisis de vulnerabilidades, debe orientarse a identificar huecos posibles en seguridad, así como realizar una periódica medición del impacto sobre los activos. Finalmente, los resultados deben ser objeto de análisis para posteriormente fortalecer los puntos flacos y así prevenir ataques o intrusiones eventuales.

[13] Ibídem.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Conocer la importancia de implementar el método Hardening en el sistema operativo de una estación de trabajo minimizando vulnerabilidades y alteración de las configuraciones de los servicios y archivos del sistema, con ello se referenciarán herramientas de análisis y protección en el hardening como son Antivirus, IDS, Firewall y Sniffer al igual que la criptografía. Para tal efecto y tras estudiar la información recopilada de las herramientas anteriormente mencionadas, se realizará el *aseguramiento de los sistemas computacionales de la empresa sitiosdima.net,* con lo cual se pone en conocimiento la importancia de asegurarlos y protegerlos.

5.2 OBJETIVOS ESPECIFICOS

- Conocer en que consiste el método Hardening y sus estrategias de aplicabilidad, incluyendo que actividades técnicas se deben tener en cuenta para realizar su debida implementación.

- Estudiar la implicación que tiene la implementación del hardening en un sistema operativo Windows en pro de mantener la integridad del sistema.

- Analizar en que reside el concepto de defensa en profundidad, su estructura y descripción del proceso de aplicación en lo que puede ser un método de protección frente a un ataque informático.

- Identificar herramientas que permiten explorar los puertos abiertos, que proceso se ejecuta en el sistema a través de éstos y cuales podrían ser un punto de entrada para un usuario malicioso.

- Identificar el concepto y la importancia que tiene el Firewall a nivel protección contra intrusiones, la adecuada configuración, activación, actualización y su variedad de opciones de servicios y limitaciones.

- Analizar las características de que disponen herramientas como Antivirus, IDS, contraseñas, criptografía y sniffers en materia de seguridad de un sistema de cómputo, en especial si se está conectado a la red.

- Estudiar políticas generales de seguridad informática, sus elementos y algunos parámetros a tener en cuenta en un aseguramiento tecnológico.

6. MARCO TEÓRICO

Con base al tema a tratar y el planteamiento a exponer en el marco teórico es clave definir previamente el concepto de administración.

De acuerdo con la definición de derecho de Robbins[14], la administración "consiste en coordinar las actividades de trabajo de modo que se realicen de modo eficaz". Según su concepto, la eficiencia "consiste en obtener los mayores resultados con la mínima inversión. Como los gerentes tienen recursos escasos (de personas, dinero y equipo) se preocupan por aprovecharlos eficientemente… la eficacia se define como hacer las cosas correctas… la mala administración es el resultado de ineficiencia y la ineficacia"[15]

La administración en general cuenta entre sus premisas con el objetivo de dar sentido a las diversas decisiones que deben considerar las organizaciones para la formulación de una estrategia que les permita responder y asignar de manera óptima los recursos humanos, financieros y de TI.

El ciclo básico de la administración, de acuerdo con Thompson[16] es: "planear, organizar, dirigir, ejecutar y controlar en su diseño más simple". Esta definición de Thompson, es una propuesta que zanja los pareceres de varios autores. Según su definición, en la primera etapa, la de la planeación, es cuando se debe realizar la selección del sistema operativo. Esta elección tendrá un profundo impacto en el desempeño de la organización, ya que con ella se genera un costo de propiedad, lo que determina la conveniencia de poseer y mantener o bien arrendar el software y/o hardware para su centro de datos.

---

[14] ROBBINS, Stephen P.2005. Administración. Editorial: Pearson –Prentice Hall - Educación. p. 7. Disponible en: http://bit.ly/1W2hlb3

[15] Ibídem.

[16] THOMSON, Ivan. Definición de Administración. {En línea}. {9 de Mayo de 2015}. Disponible en: (http://www.promonegocios.net/administracion/definicion-administracion.html).

En la práctica diaria se aprecia como el centro de datos opera como una especie de departamento encargado de administrar los recursos de TI con que se cuenta para proveer los servicios informáticos que requiere el personal de una organización. En este sentido se debe maximizar el uso, por lo tanto aprovechar los equipos de cómputo que tiene, evitando sub-utilizarlos (eficiencia, medios) para lograr sus metas (eficiencia, fines).

Sánchez Saldívar[17] destaca como en esta perspectiva, el administrador del centro de datos pasa a ser el administrador casi absoluto de los bienes informáticos, buscando la forma de aprovechar mejor los recursos de equipo de cómputo con que cuenta, "específicamente buscar la manera de robustecer la seguridad de los sistemas operativos que soportan las aplicaciones críticas de la empresa o dependencia gubernamental como parte de un esquema más complejo de seguridad en las TI."[18].

El hardening o robustecimiento puede entenderse como una "técnica compuesta por un conjunto de actividades llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de éste" [19]. Según Castro, para sacarle el mayor partido es preciso identificar las ventajas de un sistema operativo capaz de soportar y administrar de manera adecuada los recursos de memoria y procesos por medio del hardening mejorando la seguridad del mismo.

[17] SÁNCHEZ ZALDÍVAR, Omar Jonathan Cyprian. 2009. Desarrollo de una guía para selección y endurecimiento (hardening) de sistemas operativos para un centro de datos. Esime. Ciudad de México. Octubre de 2009. Disponible en: docplayer.es/1071875-Instituto-politecnico-nacional.html
[18] Ibídem, p. 57
[19] Op. Cit. Castro. 2012.

6.1 RECONOCER EL ENTORNO A PROTEGER

“No hay retorno de inversión más real que conocer el entorno que intentamos proteger, su comportamiento y particularidades”, según Marino del Río[20]. Según el autor, la clave para asegurar los sistemas informáticos pasa por un conocimiento preciso del funcionamiento de la organización.

Establecer los papeles fundamentales dentro de la organización, permite conocer el comportamiento de los activos, así como sus relaciones y dependencias.

> “¿Quién es el owner?, desde donde se gestiona y quién lo hace. Los procesos de negocio que se ejecutan y cuál es su resultado, la performance de los mismos y aquellas situaciones que todos conocen y nadie resuelve (porque de esas hay siempre). Las fuentes antes mencionadas (best practices) nos darán un buen resultado si son validadas y testeadas por las personas claves, tanto a nivel técnico (verificación técnica) como de negocio (validación y aprobación)”[21].

Según el autor, de no contarse con una confiable valoración de los activos, se pueden destinar inversiones en sectores que no ofrecen el menor impacto en los objetivos del negocio. “Lo mismo podría suceder en un proyecto de gestión de vulnerabilidades o de hardening, y todo se basa en desconocer el valor de los activos y su impacto en el cumplimiento de los objetivos de negocio. Saber cómo funciona la organización, desde sus sistemas”.[22]

---

[20] DEL RIO, Mariano M. La importancia de conocer el entorno a proteger {En línea}. {4 de Abril de 2015}. Disponible en: (https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/la_importancia_de_conocer_el_entorno_a_proteger?realLang=fr).

[21] Ibídem.

[22] Ibídem.

6.2 ROBUSTECERSE O MORIR

Sin caer en los alarmismos, Martínez Rodríguez[23] advierte cómo “todos los sistemas son susceptibles de ser atacados”. Martínez asegura que la importancia de los datos contenidos, pueden convertirse en el foco de “mafias, rivales o espionaje industrial, entre otras amenazas”.

Además de la posibilidad de robos o chantajes, ahora hay otros riesgos como secuestrar terminales para convertirlas en emisores de spam, o bien para minar bitcoins, “albergar pornografía o malware, o simplemente servir de pivote desde el que cometer “cibervandalismo” a través de Internet, y que los dedos nos apunten a nosotros”[24].

La pregunta clave que plantea el autor es: “¿qué tareas se han tomado con el fin de reducir la incidencia de eventuales ataques o incidentes informáticos?”.

> “Pensamos que cuando conectamos una máquina que da un servicio a Internet, el sistema operativo ya es seguro por el mero hecho de actualizar los parches y ponerle un “antivirus”. Parece que el objetivo de Steve Jobs, en el que un usuario desempaqueta un producto Apple, que lo enchufas y ya funciona, es el mensaje que los trabajadores de departamentos de sistemas y de desarrollo, dejando para después el trabajo de la securización de dichos sistemas”.

[23] MARTÍNEZ RODRÍGUEZ, Lorenzo. {En línea}. {25 de Junio de 2015}. La importancia del bastionado de sistemas. Disponible en: (https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/importancia_bastionado_sistemas).

[24] Ibídem.

Según Martínez Rodríguez, la lucha contra los ataques que llegan día a día, no es algo estático. Las medidas y las mejoras en la seguridad tienen que implantarse de manera continua.

En otro artículo, de mayo de 2015, Martínez Rodríguez menciona que la formación de los empleados, así como su control en el empleo de prácticas confiables, es crucial para endurecer la seguridad de los sistemas.

“Estoy de acuerdo en que para poder proteger, hay que saber atacar. Es decir, que para auditar si los sistemas de tu organización están seguros, tener conocimientos de pentesting es algo imprescindible En segundo lugar, Análisis Forense. O sea que nos interesa poder identificar, una vez que hemos tenido un incidente de seguridad, cómo y cuándo ha pasado, y cuál ha sido el alcance”[25].

Del Río por su parte plantea que en el último lugar, en la última línea de defensa, están la protección de sistemas operativos, la configuración segura de servicios, la fortificación de infraestructuras, las buenas prácticas de seguridad en dispositivos móviles, monitorización de sistemas y redes… “En general, tener conocimientos sobre cómo ponerle las cosas más difíciles a los malos, nos interesa menos que ponernos en el lugar de un supuesto atacante”.[26]

[25] MARTÍNEZ RODRÍGUEZ, Lorenzo. 2015b. Si no te esfuerzas en proteger tus sistemas constantemente ¿por qué te quejas cuando comprometen tu seguridad?. Disponible en: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Esfuerzate_proteger_tus_sistemas_constantemente

[26] Op. Cit. Del Río. 2014.

“En definitiva, quizás coincidimos en el diagnóstico pero no en su solución, porque ello depende de cada organización, su cultura, apetito de riesgo, las personas que la integran. Sin embargo, es difícil pensar en un programa de ciberseguridad efectivo sin el involucramiento de la Alta Dirección, los líderes de la organización y el personal clave de los procesos y activos que estén involucrados. Aquellos que cuenten con este escenario, sin dudas estarán ante una organización con la madurez necesaria para que las inversiones sean más efectivas y los resultados generen un verdadero valor agregado, en un mismo camino y hacia un mismo sentido.”

7. DESCRIPCIÓN GENERAL

En el desarrollo de la presente monografía (Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net), se ha planeado el análisis de las estrategias de seguridad que se emplean en la empresa sitiosdima.net como elemento fundamental de contraste respecto a las posibles vulnerabilidades a descubrir. En qué medida son importantes ciertos procesos de aseguramiento donde se logre concebir un estado de seguridad confiable para la organización.

Se decide realizar el análisis y estudio de una empresa real como sitiosdima.net debido a las posibilidades que puede brindar al realizar pruebas y constatar hipótesis. Con base a esto se quiere implementar un proceso de verificación de actualizaciones de los sistemas operativos y aplicaciones de los equipos de cómputo, igualmente se generará un proceso de verificación de estado de funcionalidad de las aplicaciones proyectada a practicar técnicas de vulnerabilidad en aplicaciones para lograr evitar accesos y escalamiento de privilegios a los sistemas operativos.

El Hardening es una ayuda indispensable que pretende evitar bastantes inconvenientes a los administradores del sistema. Como se verá más adelante, algunas ventajas que ofrece el Hardening y una de las más importantes es la disminución de incidentes de seguridad. También el hecho de brindar mejoras en el rendimiento tras eliminar cargas inútiles en el sistema como programas innecesarios, entre otros. Para Burguan "una función monousuario del sistema es más seguro que una multiusuario, ya que solo se tiene que controlar un usuario. La reducción de los ataques normalmente incluye la desinstalación de software innecesario y desactivación o eliminación de usuarios innecesarios"[27]

[27] BURGUAN, Iliana. 2014. Hardening de windows. Universidad técnica particular de Loja. Quito, Ecuador. Disponible en: https://ilianaburguan.files.wordpress.com/2010/01/taller2.doc

Uno de los principales conceptos que se deben dejar en firme respecto a la labor del robustecimiento o hardening, es la imposibilidad de hacer invulnerables a los equipos. El propósito de la implementación del hardening de sistemas, “es eliminar el mayor número de riesgos de seguridad como sea posible”[28].

> *“Muchos se preguntarán si es posible realizar la tarea de incrementar la seguridad mediante hardening a un equipo basado en la plataforma MS Windows; la respuesta es “sí”. Ya se ha comentado que la seguridad y confiabilidad de un sistema dependen en gran medida de cómo sea administrado”[29].*

> *“El proceso comienza desde el momento de decidir el uso que tendrá el equipo, ya sea como estación de trabajo, servidor de dominio, servidor de impresión, equipo Standalone, etcétera. “Los puntos anteriores son de vital importancia para el momento de la instalación, ya que recordemos que es una muy mala práctica realizar instalaciones por default, debido a que se incluye gran cantidad de programas que no serán de utilidad para los fines del servidor, por ejemplo si no se tendrá una página Web entonces para qué instalar el IIS, los juegos, etcétera”[30].*

Según Astorga, lo que deba o no estar instalado “dependerá del uso del equipo, mejor el enfoque estará en realizar el endurecimiento en las configuraciones. Ligado a esto estará el realizar las debidas actualizaciones del sistema operativo y sus componentes”[31].

---

[28] Ibídem.
[29] ASTORGA, Agustín. Hardening de un sistema MS Windows. {En línea}. {9 de Enero de 2015}. Disponible en: (http://esemanal.mx/2006/11/hardening_de_un_sistema_ms_windows/).
[30] Ibídem.
[31] Ibídem.

Astorga concluye que “cuando se habla de servidores en producción no es recomendable aplicar actualizaciones de manera automática, ya que en ocasiones salen parches los cuales contienen bugs con los cuales se estarían generando más problemas de los que se pretende solucionar”[32].

7.1 QUÉ ES HARDENING

Al instalar software, generalmente éste proceso se realiza con múltiples opciones que están configuradas por defecto. El propósito es alcanzar la adaptación eficaz a la más posible cantidad de entornos y de ésta manera hacer más cómoda la ejecución y puesta en marcha, desde luego, el objetivo que se busca es la usabilidad.

Es por ello que no es extraño toparse con usuarios y claves de contraseñas generadas automáticamente, así como puertos abiertos, componentes y controladores que dependiendo el entorno pueden o no ser requeridos en ejecución. En sí, esto se convierte en un tema de gran importancia para la seguridad de uno de los activos más importantes de cualquier organización, la información. Aquí es donde entra a operar el hardening, pues se requiere reducir el nivel de riesgo al cual esté expuesto el sistema mediante la detención de servicios y cambio de valores por defecto, entre otras medidas que se deben implementar.

Aunque el Hardening es un método el cual implementa múltiples estrategias en su aplicabilidad, es claro que su aplicación “debe ser personalizado y adecuado a cada entorno en específico en función de sus necesidades para que las configuraciones de seguridad no penalicen la operación. Para poder implementar esta estrategia se necesita que la organización documente puntualmente las funcionalidades que

[32] Ibídem.

estén permitidas y aquellas que están denegadas y describa los pasos para implementar dichas configuraciones".[33]

Para lograr generar un estado aceptable de protección empleando Hardening se debe analizar diferentes aspectos técnicos y humanos a la hora de implementarlo. El Hardening se manifiesta en los sistemas operativos de forma preventiva y se debe aplicar igualmente el concepto de defensa en profundidad, esto con el fin de limitar al atacante si este ha logrado avanzar en el ataque.

7.1.1 Actividades técnicas que se deberían tener en cuenta frente al Hardening,

- Configuraciones seguras. Esta actividad es importante y clave a la hora de implementar Hardening en un sistema operativo, ya que la mayoría de intrusiones son facilitadas por la mala gestión técnica o la no existencia de políticas de seguridad en los sistemas operativos. Los permisos a usuarios y servicios mal configurados fortalecen el acceso a información que pueda facilitar aún más la intrusión, por lo cual una adecuada configuración y un escalamiento controlado puede evitar que el atacante tome control total del sistema operativo manipulándolo de forma que se pueda acceder a otros equipos en red.

La asignación de contraseñas seguras en su longitud y dificultad es importante igualmente para generar límites de acceso, se puede asignar tanto en el inicio del sistema operativo como en aplicaciones y cuentas de usuario, con esto se fortalece las autenticaciones de usuarios al sistema operativo al igual que limita a programas maliciosos como virus a tomar control del sistema operativo.

[33] ACOSTA, David. Estandares de Configuración Segura Hardening en pci. {En línea}. {09 de Marzo de 2015}. Disponible en: (http://www.pcihispano.com/estandares-de-configuracion-segura-hardening-en-pci-dss/).

- Bastionado de sistemas (hardening). Tarlogic define el bastionado de sistemas o hardening como “la protección de un sistema o conjunto de sistemas informáticos mediante la aplicación de configuraciones de seguridad específicas para prevenir ataques informáticos, contener la elevación de privilegios, mitigar el robo de información, y obtener la trazabilidad necesaria para analizar un ataque en el caso de que haya sucedido”[34].

> “Un bastionado de sistemas consiste en realizar una auditoría de seguridad o un test de intrusión sobre un equipo informático para a continuación definir las recomendaciones necesarias, a nivel de requisitos de seguridad, configuración, módulos y aplicaciones externas necesarias con las que dotar al sistema de las máximas garantías de protección en su configuración base”[35].

El bastionado de sistemas requiere la creación de una línea base de seguridad para las organizaciones, aplicando modificaciones de configuración y recomendaciones a una maqueta del sistema informático que será desplegado en la empresa para obtener protección frente a malware, ataques dirigidos, configuración de servicios y antivirus, revisión de permisos y ACLs del sistema, aplicación de directivas a través de GPOs para restringir privilegios. Un hardening adecuado no debe interferir en la usabilidad del sistema pero lo protegerá de la mayoría de amenazas y ataques informáticos.[36]

“A continuación, ejemplos de distintas líneas base de seguridad que pueden ser definidos en las organizaciones:

[34] TARLOGIC. Bastionado de sistemas (hardening). {En línea}. {4 de Julio de 2015}. Disponible en: (https://www.tarlogic.com/servicios/bastionado-de-sistemas-hardening/).
[35] Ibídem.
[36] Ibídem.

- Línea base de seguridad para usuarios: Protección de la configuración del puesto de trabajo Windows de los usuarios de la empresa para evitar ataques informáticos y manipulación del terminal.

- Línea base de seguridad para usuarios VIP: Determinados usuarios en función de su rol dentro de las empresas tienen requisitos de seguridad, privacidad y confidencialidad diferentes según la información a la que tienen acceso.

- Línea base de seguridad para servidores: Bastionado de sistemas dependiendo del rol que desempeñan (Directorio activo, servidor web, servidor de bases de datos...)

Durante el proceso de definición de una línea base de seguridad para el proceso de hardening se estudia el software utilizado en el sistema, tanto interno de la empresa como externo, y se analiza el perfil de los usuarios para que las protecciones se adecuen al uso de sistema. Estas medidas de seguridad afectarán también a los permisos de las tareas autorizadas paquetes ofimáticos como Microsoft Office".[37]

7.2 IMPLEMENTACIÓN EN SISTEMAS OPERATIVOS WINDOWS

El hardening en un equipo personal o de uso empresarial pasa por proteger los datos personales y la información de carácter privado para la empresa. Mediante éste proceso se quiere eliminar en gran medida los medios de ataque existentes en el sistema mediante parches que subsanen vulnerabilidades y desactivar servicios no esenciales. El hardening implementado en un sistema implica distintas estrategias por aplicar, dependiendo del entorno y usabilidad, el nivel de protección

[37] Ibídem.

requerido puede variar. A continuación se mencionan algunas de las medidas básicas a implementar en sistemas Windows.

La implementación de sistemas operativos Windows hacen parte de un importante procedimiento a la hora de aplicar seguridad en una corporación, los sistemas Windows son más propensos a sufrir ataques informáticos por la gran variedad de códigos malicioso que existe en la red o programas ya desarrollados para este sistema operativo. La ejecución de este sistema se debe basar en el concepto de defensa en profundidad el cual se realiza para asegurar el sistema base para minimizar una intrusión informática, estas culminaciones hacen que por medio de ajustar configuraciones por defecto o servicios que no son utilizados fortalezcan la seguridad desde la base del sistema operativo.

Por lo anterior se debe implementar teniendo en cuenta la disponibilidad, confiabilidad e integridad del sistema, lo cual se debe mantener en el tiempo por medio de actualizaciones, pruebas de penetración y auditorias de sistemas.

La configuración de usuarios del sistema, el cifrado de datos, el control de los servicios y la verificación de fallos de las aplicaciones o programas que se administren deben ser analizados para generar compatibilidad y seguridad en el momento de implementarlos en sistemas operativos Windows.

7.2.1 Parche automáticamente Microsoft Windows.

> "Las actualizaciones importantes ofrecen ventajas significativas, como una mayor seguridad y confiabilidad. También puede configurar Windows para que instale automáticamente las actualizaciones recomendadas, que pueden solucionar problemas que no son críticos y ayudar a mejorar la experiencia del usuario. Las actualizaciones opcionales no se descargan ni se instalan automáticamente".[38]

7.2.2 Otras Medidas de Seguridad.

- Utilice contraseñas seguras o pasar frases para todas las cuentas de usuario de Windows en su PC.

- Utilizar y mantener correctamente un buen software anti-virus, y, opcionalmente, software anti-spyware.

- Abstenerse de dar apertura a archivos adjuntos que puedan venir en correos electrónicos sospechosos. Tampoco se debe responder a solicitudes sospechosas.

- Si no lo está utilizando, deshabilitar el archivo de Windows y el servicio Compartir impresoras.

- Desactive las cuentas de usuario que no sean necesarios.

- Bloquear la pantalla de su PC cuando usted se aleja y apagar el ordenador cuando se le ha ido por más de 6 horas.

7.2.3 Instalación de Sistema Operativo. Es importante cometer un sistema de seguridad desde el inicio de la instalación de un sistema operativo, por lo cual, la

[38] MICROSOFT. Amenazas y Contramedidas. {En línea}. {3 de Abril de 2015}. Disponible en: (https://technet.microsoft.com).

actividad de Hardening fortalece adecuadamente la configuración por defecto que se instala por primera vez en un equipo. Adicional a esto, se debe tener en cuenta asegurar parámetros de red, actualización del sistema y configuraciones por defecto que puedan vincular una vulnerabilidad al sistema operativo.

Los archivos y carpetas deben estar con sus permisos exactos según el uso que se le dará, regularmente los permisos de solo lectura se aplican para minimizar alteración de carpetas importante como archivos de configuración que pueda afectar un servicio del sistema operativo, como ejemplo se puede mencionar el archivo HOST el cual contiene los parámetros de validación de dominios locales, una alteración de este archivo puede generar un ataque de PHARMING o DNS-SPOONFING, modificando las direcciones IP que llaman cada dominio al ser solicitado en el navegador; Esto con el fin de re direccionar el usuario a un sitio falso que capturara sus credencias o información personal, como se ve, una mala configuración o deficiencia de permisos en archivos puede vulnerar información y comprometer el sistema operativo de forma importante e impactante para el funcionamiento y eficiencia de equipo.[39]

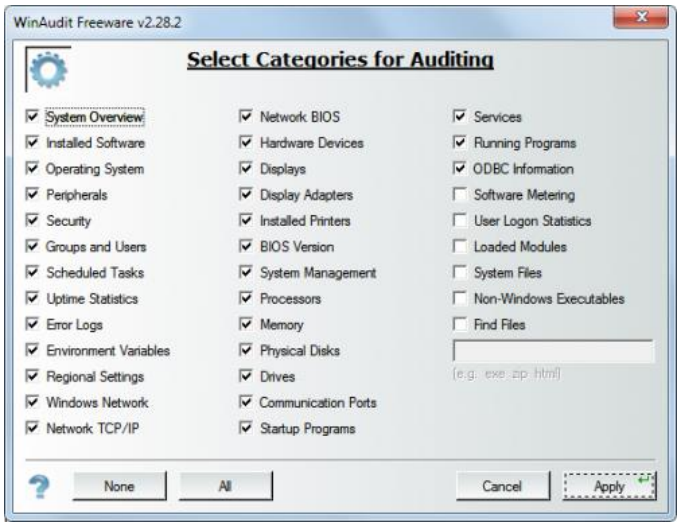
7.2.4 Auditorias del sistema. Las auditorías a nivel del sistema operativo deben ser obligatoriamente aplicada para saber qué está pasando en el sistema, por lo anterior generar políticas de seguridad respecto al tema de auditoria es importante para analizar y diseñar estrategias que permitan mitigar problemas que generen pérdida de control y gestión del sistema operativo.

En el mercado existe gran cantidad de herramientas que brindan la posibilidad de realizar auditorías técnicas al sistema operativo, éstas aplicaciones brindan innumerables posibilidades de análisis facilitando de ésta manera realizar una tarea bastante confiable por parte del auditor. Cada día son más populares las Técnicas

[39] G_SMARTEKH. Qué_es_hardening. {En línea}. {12 de Enero de 2015}. Disponible en: (http://blog.smartekh.com).

de Auditoría Asistidas por Computador (TAAC'S), estas herramientas dan la posibilidad al auditor realizar tareas como; validar las rutinas de procesamiento de transacciones, detectar y controlar errores, detectar cambios anormales en el sistema, alertar sobre situaciones fraudulentas entre muchas más posibilidades. En el ANEXO A, se puede apreciar un ejemplo de Auditoría Técnica el cual fue realizado con el software WinAudit de Microsoft, aplicación con licencia gratuita.

Figura. 1. Aplicación para Auditoría de Sistemas

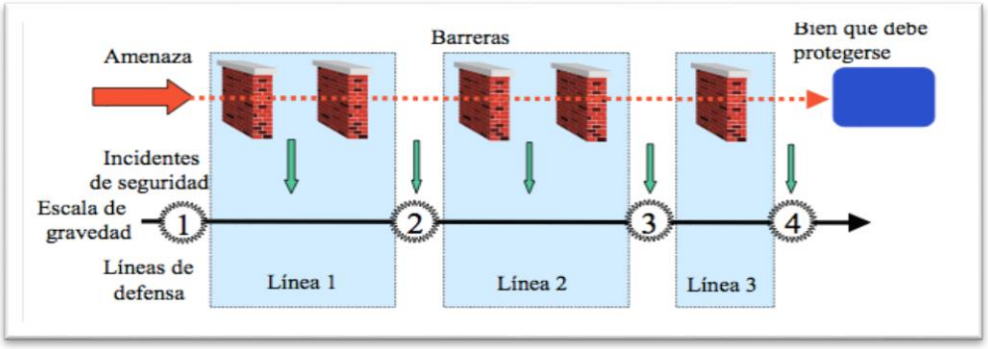


Fuente: http://adnfriki.com/saber-que-componentes-hardware-tiene-tu-pc/

7.3 DEFENSA EN PROFUNDIDAD DE LA SEGURIDAD INFORMATICA

Los ataques direccionados son ataques con los que se logra tener un alto nivel de intrusión por su estructura y técnicas utilizadas, con base a esto es importante implementar un aseguramiento de los sistemas operativos aplicando el concepto de seguridad en profundidad. A continuación se verá un modelo tomado de la Agencia Nacional de seguridad de Sistemas de Información de Francia, donde se aprecia claramente el concepto de defensa en profundidad en un gráfico que limita y define cada instancia de protección frente a un ataque informático.

Figura. 2. Procedimiento de identificación de las líneas de defensa



Fuente: http://www.ssi.gouv.fr/archive/es/confianza/documents/methods/mementodep-V1.1_es.pdf

En el anterior grafico se puede describir claramente el proceso de protección que es estructurado en el concepto de defensa en profundidad, se denomina líneas a cada nivel de seguridad que es planteado frente a un fenómeno de amenaza, cada uno de estos fenómenos dependiendo de su agresividad es tratado de manera diferente y filtrado en cada línea de seguridad que se manifiesta al tener un ataque informático.

Cada amenaza se clasifica según su impacto y se define en una escala de gravedad donde se puede afirmar la penetración del ataque según la línea de defensa que vulnera, con esto se puede analizar qué tipo de ataque, su efectividad, información del mismo y la forma de vulnerar las líneas de defensa.

Las líneas que componen la defensa en profundidad pueden comportarse estáticas o dinámicamente, esto hace flexible las políticas de seguridad y elementos de seguridad que se implementen en cada línea de seguridad, los usuarios hacen parte importante en este proceso ya que estos identifican consciente o inconscientemente los problemas de seguridad que puedan causar daños o no. Para lo anterior es importante tener claras diferentes procedimientos donde se incluyen registro de actividades, registro de incidentes y alertas de posibles intrusiones que permitan

tener un marco claro de cada ataque, esto con el fin de determinar y proteger el activo a proteger.

Este modelo de defensa es de gran ayuda a la hora de protegerse de vulnerabilidades de día 0, ya que por ser códigos que se explotan para tener control de los sistemas operativos el aseguramiento en líneas de seguridad ayuda a minimizar el ataque y evitar que se propague causando daños significativos.

Los exploit de día 0 son aquellos que no cuentan con una solución inmediata frente a un problema de seguridad, por ello se hacen tan peligrosos, estos al penetrar la primera línea de seguridad dependiendo de su configuración y código malicioso puede lograr acceso al sistema manipulándolo a la medida del atacante, para ello la línea de seguridad basada en herramientas entra a ser la que resaltaría su funcionalidad frente al ataque, estas herramientas puede ser firewall o IDS los cuales pueden interactuar y bloquear el ataque de manera proactiva.[40]

7.4 CIERRE DE PUERTOS ABIERTOS

Un sistema operativo Windows, tras la instalación, puede llegar a tener algunos puertos abiertos. “Estos puertos son necesarios para que el sistema funcione correctamente, mientras que otros no. Estos puertos pueden representar un riesgo para la seguridad, ya que todos los puertos abiertos en un sistema podrían ser un punto de entrada para un usuario malicioso”[41].

[40] DCSSI. La defensa en profundidad aplicada a los sistemas de información. {En línea}. {19 de Mayo de 2015}. Maubourg: s.n.2004.

[41] OSFLASH (2015) Mejorar Seguridad de Windows cerrando puertos abiertos. Disponible en: http://www.osflash.com/mejorar-seguridad-de-windows-cerrando-puertos-abiertos/

"*Un puerto, básicamente, permite la comunicación desde o hacia el dispositivo. A continuación se hará un breve recuento de algunas herramientas necesarias para identificar y evaluar los puertos abiertos en el sistema Windows"*.[42]

Los ataques informáticos remotos regularmente son explotados por diferentes técnicas de intrusión, estas técnicas son realizadas regularmente definiendo una traza de conexión por medio de los protocolos disponibles en la red atacada o equipo de cómputo, por ello la definición de limitaciones en equipos de seguridad perimetrales es una política de seguridad importante y prioritaria.

Los puertos regularmente están disponibles por defecto para diferentes servicios, ahí está la clave de definir qué servicios se harán disponibles y cuáles no, al tener claro esto se debe configurar los equipos de seguridad y cerrar los que no se utilizarán. Regularmente no es suficiente cerrar puertos para tener seguridad optima, por ello se debe practicar procesos de aseguramiento que minimicen y hagan más difícil el identificar que puerto responde a solicitudes, para ello, se practica cambiar el número de puerto del servicio o limitar el direccionamiento de direcciones IP al igual que redes que interactúen con la red o equipo de cómputo.

Las vulnerabilidades que presenta el no asegurar los puertos o no cerraros pueden llegar a tener dificultades tales como la instalación de software malicioso de manera silenciosa en el equipo o equipos que estén conectados a la red, los troyanos o accesos de Shell son los más utilizados en los ataques informáticos y los puertos más comunes son los de correo electrónico SMTP y Webserver HTTP utilizados actualmente por BOTNETS.[43]

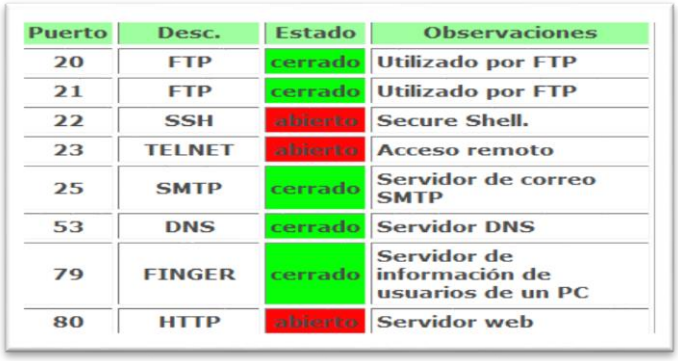
---

[42] B1NARY0. Cierre de Puertos Abiertos. {En línea}. {2 de Mayo de 2015}. Disponible en: (http://www.b1nary0.com.ar).

[43] FUNDACIONCTIC. Medidas de seguridad básica: Los puertos de tu router. {En línea}. {15 de Mayo de 2015}. Disponible en: (http://www.fundacionctic.org/sat/articulo-medidas-de-seguridad-basicas-los-puertos-de-tu-router).

7.4.1 CurrPorts.

Figura. 3. Escaneo de puertos



Puerto	Desc.	Estado	Observaciones
20	FTP	cerrado	Utilizado por FTP
21	FTP	cerrado	Utilizado por FTP
22	SSH	abierto	Secure Shell.
23	TELNET	abierto	Acceso remoto
25	SMTP	cerrado	Servidor de correo SMTP
53	DNS	cerrado	Servidor DNS
79	FINGER	cerrado	Servidor de información de usuarios de un PC
80	HTTP	abierto	Servidor web

Fuente: http://www.pelechano.com/wp-content/uploads/2011/08/puertos.png

"Es una aplicación que permite saber cuáles son los puertos que están siendo utilizados por las distintas aplicaciones. Esta herramienta muestra en un listado los puertos TCP y UDP en uso".

> "Permite realizar diversas acciones sobre estos, como conocer información detallada sobre cada uno, cerrar la conexión o aniquilar el proceso que usa un puerto determinado. Otra función interesante es la posibilidad de realizar un informe en formato HTML con los datos de todos los que estén abiertos. El usuario puede seleccionar la información que mostrará las columnas del programa. Desde el menú opciones se pueden habilitar y deshabilitar elementos. Los datos que puedes conocer son la dirección IP remota a la que accede el equipo, los puertos de origen y de destino, el tipo de apertura, y mucho más".[44]

El programa muestra el nombre del proceso y la identificación, puerto local, el protocolo y el nombre del puerto local, entre otros. "Los más importantes son el número de puerto, el nombre del puerto local y el ID del proceso"[45].

[44] UPTODOWN. Conoce qué puertos TCP y UDP utiliza tu equipo. {En línea}. {3 de Julio de 2015}. Disponible en: (http://currports.uptodown.com).

[45] OSFLASH (2015) Mejorar Seguridad de Windows cerrando puertos abiertos. Disponible en: http://www.osflash.com/mejorar-seguridad-de-windows-cerrando-puertos-abiertos/

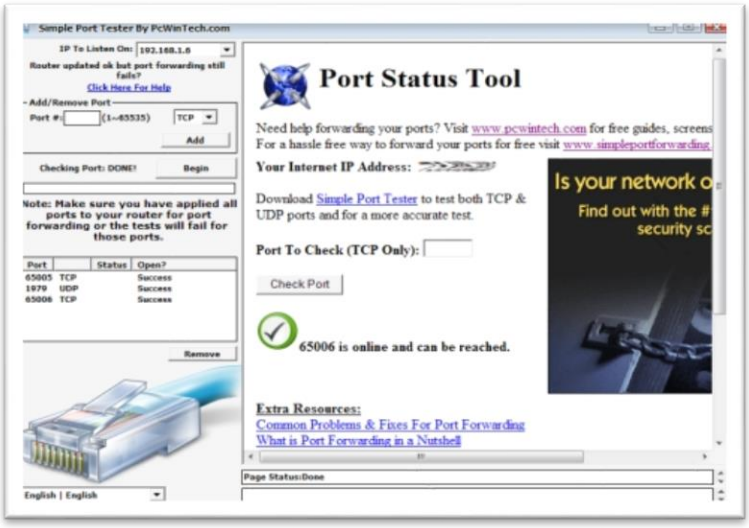
> “Con el ID del proceso se puede echar un vistazo en el Administrador de tareas de Windows para tratar de vincularlo a un proceso que se ejecuta en el sistema. A menudo hay varias sugerencias o posibilidades. En ocasiones no es necesario deshabilitar un servicio, es suficiente con bloquear el puerto en el firewall”[46].

7.4.2 Simple Port Tester. Este programa *“permite comprobar si un puerto determinado o un rango está abierto, cerrado, tanto en TCP como en UDP. El programa es muy útil, por ejemplo, para comprobar si un puerto está abierto, en los programas de intercambio P2P, como uTorrent, Emule, etc, evitando de ésta forma problemas de seguridad”*.[47]

La aplicación tiene una interfaz amigable, lo que hace simple su uso. En síntesis, se selecciona la IP en uso privada que aparece desplegada en la lista del programa, para después identificar “el puerto o rango de puertos que se quiere comprobar, su protocolo y hacer clic en empezar. Se abrirá un panel en la parte derecha con la IP en éste caso pública y el estado del puerto”[48].

[46] RHO5223. Mejorar la seguridad de Windows mediante el cierre de puertos abiertos {En línea}. {10 de Julio de 2015}. Disponible en: (http://geexone.blogspot.com.co/2010/04/mejorar-la-seguridad-de-windows.html).
[47] CASTILLA, José. Comprueba qué puertos tiene abiertos {En línea}. {5 de Abril de 2015}. Disponible en: (http://www.softzone.es).
[48] Ibídem.

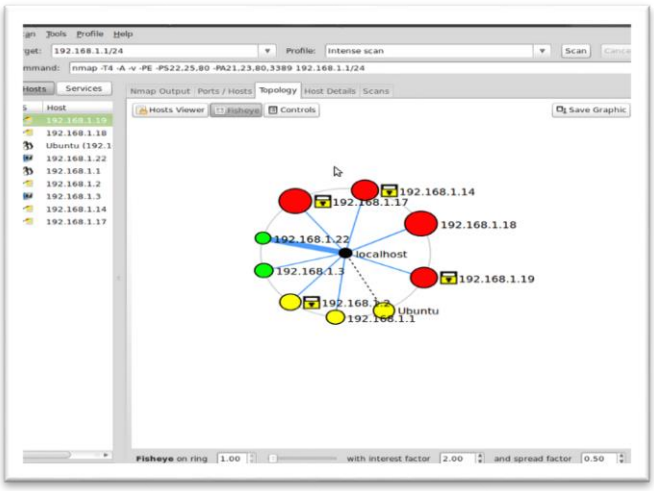
Figura 4. Software para verificar estado de puertos



Fuente: http://cdn6.portalprogramasnet.com/imagenes/programas/es/757/9757_1.jpg

7.4.3 Zenmap

Figura 5. Escáner Multiplataforma de Interfaz Gráfica



Fuente: http://michaelhumiston.com/wp-content/uploads/2011/03/zenmap2.png

"Zenmap es la Nmap Security Scanner GUI oficial. Es una multiplataforma (Linux, Windows, Mac OS X, BSD, etc.) la aplicación gratuita y de código abierto que tiene como objetivo hacer Nmap fácil de usar para principiantes mientras que proporciona características

avanzadas para los usuarios de Nmap experimentados. Frecuentes exploraciones utilizadas se pueden guardar como perfiles para que sean fáciles de ejecutar repetidamente. Un creador de comandos permite la creación interactiva de líneas de comandos de Nmap. Los resultados del análisis se pueden guardar y ver más tarde. Los resultados del análisis guardado, se pueden comparar entre sí para ver qué tan diferente. Los resultados de las exploraciones recientes se almacenan en una base de datos".[49]

7.5 FIREWALL

El firewall es un dispositivo que apoya el bloqueo de conexiones entrantes y salientes de una red, esto con el fin de limitar accesos no deseados que puedan vulnerar los equipos de la red. Existen firewall de red o de host, los de red son implementados para proteger los equipos y sistemas de información de una red y los de host protegen a los equipos de cómputo o servidores directamente desde su núcleo de conexiones.

Para los equipos con firewall de host el aseguramiento tecnológico es clave ya que por medio de este se minimiza las posibles intrusiones y se bloquea accesos por medio de vulnerabilidades que afecten las aplicaciones o programas que estén en los equipos de cómputo o servidores, los firewall de host permiten por medio de reglas restringir conexiones externas a servicios y puertos del equipo, el firewall de red restringe tráfico de red y limita desde el perímetro accesos vulnerables a los sistemas.

Su configuración igualmente debe ser analizada para evitar falsos positivos los cuales podrían afectar servicios que hagan parte de la interacción con los usuarios y las aplicaciones. Existen firewall para sistemas operativos Windows y basados en Linux varia en la facilidad e interacción con el usuario final.

[49] LYON, Gordon. Obtaining, Compiling, Installing, and Removing Nmap. {En línea}. {12 de Mayo de 2015}. Disponible en: (https://nmap.org).

> “Cada ordenador que se conecta a internet (y, básicamente, a cualquier red de ordenadores) puede ser víctima del ataque de un hacker. La metodología que generalmente usan los hackers consiste en analizar la red (mediante el envío aleatorio de paquetes de datos) en busca de un ordenador conectado. Una vez que encuentra un ordenador, el hacker busca un punto débil en el sistema de seguridad para explotarlo y tener acceso a los datos de la máquina”[50].

De acuerdo con CCM, existen varias razones para considerar que “esta amenaza es aún mayor cuando la máquina está permanente conectada a internet”, a saber:

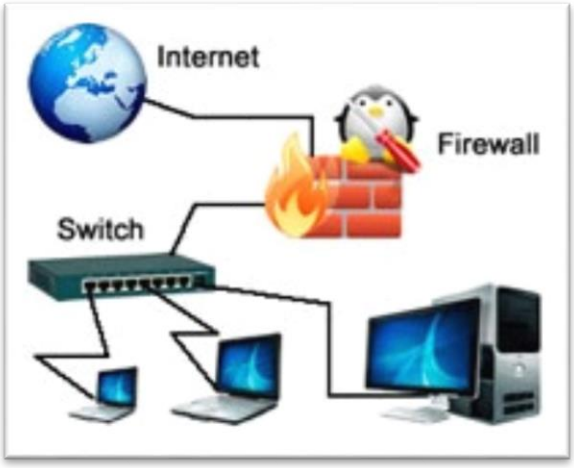
> *“- Es probable que la máquina elegida esté conectada pero no controlada.*
>
> *- Generalmente, la máquina conectada que se elige posee un ancho de banda más elevado.*
>
> *- La máquina elegida no cambia las direcciones IP o lo hace muy ocasionalmente”*.

El autor concluye su explicación sosteniendo la necesidad de que “tanto las redes de las compañías como los usuarios de internet con conexiones por cable o ADSL se protejan contra intrusiones en la red instalando un dispositivo de protección”[51].

[50] Op. Cit. CCM, 2015.
[51] Ibídem.

7.5.1 ¿Qué es un Firewall?

Figura 6. Esquema básico de un Firewall



Fuente: http://soluciones-ip.pe/ip/wp-content/uploads/2014/07/f1.jpg

CCM define el firewall como “un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet”[52]. Según este orden de ideas, consiste en “una pasarela de filtrado que comprende al menos las siguientes interfaces de red: a) Una interfaz para la red protegida (red interna); y b) Una interfaz para la red externa”.

> *“El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:*

[52] Ibídem.

- La máquina tenga capacidad suficiente como para procesar el tráfico

- El sistema sea seguro

- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor.

En caso de que el sistema de firewall venga en una caja negra (llave en mano), se aplica el término 'aparato'".[53]

7.5.2 Configuración de Firewall de Windows. Los requerimientos y preceptos esenciales del sistema se pueden llegar a personalizar a través de cuatro opciones, cada una correspondiente a una ubicación de red. Para buscar estas opciones de configuración, se aconsejan los siguientes pasos:

"- Para abrir Firewall de Windows, haga clic en el botón Inicio y, seguidamente, en Panel de control. En el cuadro de búsqueda, escriba firewall y, a continuación, haga clic en Firewall de Windows.

- En el panel izquierdo, haga clic en Activar o desactivar Firewall de Windows. Se requiere permiso de administrador Si se le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación"[54].

[53]Ibídem.

[54] MICROSOFT (2014) Permitir que un programa se comunique a través del Firewall de Windows. Disponible en: http://windows.microsoft.com/es-co/windows/communicate-through-windows-firewall#1TC=windows-7

Figura 7. Panel de opciones en Seguridad Avanzada del Firewall Windows

Fuente: Los autores.

7.5.3 Activar Firewall de Windows. Microsoft[55] especifica que la opción de firewall en su sistema operativo adquiere de forma predeterminada el estatus de activada. “Cuando Firewall de Windows está activado, se bloquea la comunicación a través del firewall para la mayoría de los programas. Si desea permitir que un programa se comunique a través del firewall, puede agregarlo a la lista de programas permitidos. Por ejemplo, es posible que no pueda enviar fotografías en mensajes instantáneos hasta que agregue el programa de mensajería instantánea a la lista de programas permitidos”[56].

7.5.4 Bloquear todas las conexiones entrantes, incluidas las de la lista de programas permitidos.

> “Con esta opción se bloquean todos los intentos de conexión al equipo no solicitado. Esta opción se usa cuando se necesita la máxima protección en un equipo; por ejemplo, al conectarse a una red pública en un hotel o un aeropuerto, o cuando hay gusano que se está extendiendo por los equipos a través de Internet. Con esta opción no se le avisa cuando Firewall de Windows bloquea programas y se omiten los programas que figuran en la lista de programas permitidos”.[57]

[55] Ibídem.
[56] Ibídem.
[57] MICROSOFT. Descripción de la configuración de Firewall de Windows. {En línea}. {23 de Enero de 2015}. Disponible en: (http://windows.microsoft.com).

En caso de cerrarse toda conexión puede apreciarse la mayor parte de los portales mencionados. Del mismo modo se tiene la posibilidad de usar el correo y de recibir mensajes instantáneos.

“Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser la web, el correo o el IRC. Dependiendo del servicio, el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

Por ejemplo, para un servidor web, únicamente se permite la entrada por el puerto 80 (web) y puerto 21 (FTP). Además, se puede definir, que se utilice el programa de FTP únicamente desde sus instalaciones, o desde unos ordenadores concretos de sus instalaciones y/o externos.

De esta manera, la configuración y seguridad es máxima. Se puede generar un servidor, para que realice la función de firewall para toda su empresa, haciendo de puente entre la red interna de la oficina con Internet.

Al hacer de puente, permite controlar todo el tráfico que pasa a través del mismo, de este modo podemos contar con estadísticas de navegación de los usuarios de la red interna, e implementar servicios como VPN (Virtual Private Networks), DMZ (Zona Desmilitarizada) en las dos direcciones (Internet-red interna y red interna-Internet).

Gracias a este control, podemos impedir el acceso desde el exterior de cualquier persona no autorizada, se puede especificar para cada usuario, que aplicaciones de Internet puede utilizar, ya sea el Messenger, correo, web, Kazza, eMule, etc… También permite especificar, que direcciones web se pueden visualizar y cuáles no. El firewall con las aplicaciones del servidor actualizadas, nos garantiza la completa seguridad del sistema.”[58] (IP)

[58] IP, Soluciones. Firewall Cortafuegos. {En línea}. {8 de Febrero de 2015}. Disponible en: (http://soluciones-ip.pe/firewall-cortafuegos).

7.5.5 Restricciones en el Firewall. Segu.info destaca la relevancia de las tareas de los firewalls. Dentro de estas está la entrega o revocatoria de licencias o accesos a servicios, los cuáles se discriminan de acuerdo con los usuarios y la ubicación que posean:

> *- "Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina Trusted (validados). Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.*
>
> *- Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna"*[59].

En síntesis, la solicitud de accesos por parte de terceras personas, tienen generalmente el objetivo de "prestar servicios al perímetro interior de la red"[60]. En este sentido, plantea el artículo es pertinente que dichas cuentas "sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias"[61].

7.5.6 Beneficios de un Firewall. Segu.info resalta que los Firewalls "manejan el acceso entre dos redes"[62]. La publicación resalta que si dicha vinculación fuera inexistente, "todas las computadoras de la red estarían expuestos a ataques desde el exterior"[63]. En síntesis, la seguridad de la red depende del grado de complejidad requerido para vulnerar la seguridad de cada terminal dentro de la compañía.

---

[59] SEGU.INFO (2014) Firewall / Cortafuegos. Disponible en: http://www.segu-info.com.ar/firewall/firewall.htm
[60] Ibídem.
[61] Ibídem.
[62] Ibídem.
[63] Ibídem.

> “El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos”[64].

Segu.info también remarca otras motivaciones que han encumbrado el empleo de Firewalls. Una de ellas es la crisis generada por la insuficiencia de direcciones IP, dada por el límite de los caracteres y combinaciones. Esta condición ha propiciado que las intranets “tomen direcciones sin clase, las cuales salen a Internet por medio de un ‘traductor de direcciones’, el cual puede alojarse en el Firewall”[65].

“*Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda ‘consumido’ por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible*”[66].

Adicional a estas, los Firewalls tienen otras condiciones de uso, bien sean para seccionar sitios con diferentes requerimientos de seguridad o bien sea para “albergar los servicios WWW y FTP brindados”[67].

7.5.7 Limitaciones de un Firewall. Segu.info advierte como una de las dificultades más protuberantes de un Firewall, es la generación de vacíos que no se llenan y que pueden ser identificados por un hacker o un cracker.

> *“Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza*

[64] Ibídem.
[65] Ibídem.
[66] Ibídem.
[67] Ibídem.

de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original"[68].

Otro condicionamiento importante es que el firewall difícilmente logra identificar el riesgo a través de un acceso individual. En este sentido, si se descubren claves o huecos, difícilmente el sistema de control lo note.

"El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados"[69]

"Finalmente, un Firewall es vulnerable, él NO protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: "cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos. El único Firewall seguro (100%) es aquel que se mantiene apagado"[70]

7.6 VIRUS INFORMÁTICO

7.6.1 ¿Qué es un virus informático? "Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador. Aunque no todos son tan dañinos. Existen unos un poco más inofensivos que se caracterizan únicamente por ser molestos"[71].

[68] Ibídem.
[69] Ibídem.
[70] Ibídem.
[71] GCFAPRENDELIBRE. ¿Qué son los antivirus? {En línea}. {19 de Febrero de 2015}. Disponible en: (http://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_antivirus/1.do).

7.6.2 Métodos de infección. Gfcaprende[72] discrimina las variadas situaciones en las que una terminal puede resultar contaminada:

"- Mensajes dejados en redes sociales como Twitter o Facebook.

- Archivos adjuntos en los mensajes de correo electrónico.

- Sitios web sospechosos.

- Insertar USBs, DVDs o CDs con virus.

- Descarga de aplicaciones o programas de internet.

- Anuncios publicitarios falsos."[73]

7.6.3 ¿Cómo infecta un virus el computador?

De acuerdo con Gfcaprende existe una reiterada rutina que hace que una terminal resulte infectada, a saber:

> *"- El usuario instala un programa infectado en su computador. La mayoría de las veces se desconoce que el archivo tiene un virus.*
>
> *- El archivo malicioso se aloja en la memoria RAM de la computadora, así el programa no haya terminado de instalarse.*
>
> *- El virus infecta los archivos que se estén usando en ese instante.*
>
> *- Cuando se vuelve a prender el computador, el virus se carga nuevamente en la memoria RAM y toma control de algunos servicios del sistema operativo, lo que hace más fácil su replicación para contaminar cualquier archivo que se encuentre a su paso".*[74]

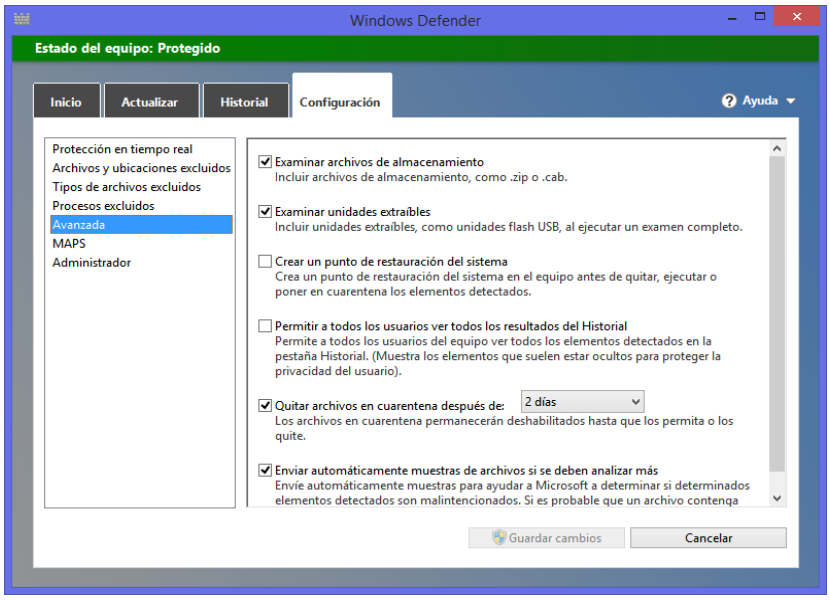
7.6.4 Antivirus. Existen dos conceptos e implementaciones, los antivirus Gateway y los antivirus de host, el primero hace referencia a la implementación en sistemas

[72] Ibídem.
[73] Ibídem.
[74] Ibídem.

de red con zonas desmilitarizadas DMZ las cuales filtran el tráfico en busca de virus o código malicioso y el antivirus de host se instala en equipos o servidores donde analiza los archivos que son descargados en busca de virus o código malicioso.

> “Los antivirus regularmente se deben configurar para ser actualizados automáticamente para que las firmas puedan ser comparadas con los nuevos códigos maliciosos que existan. La comparación de encabezados de los archivos hacen que el antivirus detecten si es malicioso o no, igualmente su comportamiento en el sistemas ya que los virus regularmente toman el comportamiento de procesos del sistema y actúan como tal, por ello regularmente se debe analizar comportamiento y efecto para determinar si es un virus o un proceso normal del sistema”.[75]

Figura. 8. Protección del Equipo Mediante Antivirus.



Fuente: Los autores.

En síntesis, un antivirus es una aplicación cuyo objetivo básico es detectar virus informáticos y brindar diferentes opciones a implementar. Por ende, es una herramienta fundamental en materia de seguridad para cualquier sistema

[75] Ibídem.

informático. La evolución de la informática trae consigo ventajas y desventajas. A la par cada instante aparece gran cantidad de amenazas lo cual exige el uso permanente de un buen antivirus que detecte y bloquee cualquier amenaza, la desinfecte y se actualice periódicamente.

Principales funciones y componentes del antivirus.

Vitriago menciona las siguientes:

Vacuna. “Es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en tiempo real”.[76]

Detector. Es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o PATH. “Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura”[77].

Eliminador. “Es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas”[78]. Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará correctamente si es adecuado y está bien configurado. Además, un antivirus es una herramienta para el usuario y no sólo no será eficaz para el 100% de los casos, sino que nunca será una protección total ni definitiva.

[76] VITRIAGO, Michael. Virus y antivirus de computadora. {En línea}. {14 de Marzo de 2015}. Disponible en: (http://www.monografias.com/trabajos94/virus-y-antivirus-pc/virus-y-antivirus-pc.shtml).
[77] Ibídem.
[78] Ibídem.

Según Vitriago, “la función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles”.
Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada.[79]

7.6.5 Clasificación de los antivirus.

Identificados por Vitriago, se mencionan a continuación las siguientes clasificaciones:

> *“- Antivirus ‘preventores’. Como su nombre lo indica, este tipo de antivirus se caracteriza por anticiparse a la infección, previniéndola. De esta manera, permanecen en la memoria de la computadora, monitoreando ciertas acciones y funciones del sistema.*
>
> *- Antivirus identificadores. Esta clase de antivirus tiene la función de identificar determinados programas infecciosos que afectan al sistema. Los antivirus identificadores también rastrean secuencias de bytes de códigos específicos vinculados con dichos virus.*
>
> *Antivirus “descontaminadores”. Comparte una serie de características con los identificadores. Sin embargo, su principal diferencia radica en el hecho de que el propósito de esta clase de antivirus es descontaminar un sistema que fue infectado, a través de la eliminación de programas malignos. El objetivo es retornar dicho sistema al estado en que se encontraba antes de ser atacado. Es por ello que debe contar con una exactitud en la detección de los programas malignos”[80].*

[79] SITIOSARGENTINA. {En línea}. {6 de Abril de 2015}. Qué es un Antivirus. Disponible en: http://www.sitiosargentina.com.ar
[80] Op. Cit. Vitriago. 2013.

7.6.6 Tipos de antivirus.

Al igual que no hay virus idénticos, tampoco hay sistemas antivirus iguales.

Vitriago identifica los tipos de sistemas antivirus así:

"- Anti espías o antispyware. Esta clase de antivirus tiene el objetivo de descubrir y descartar aquellos programas espías que se ubican en la computadora de manera oculta.

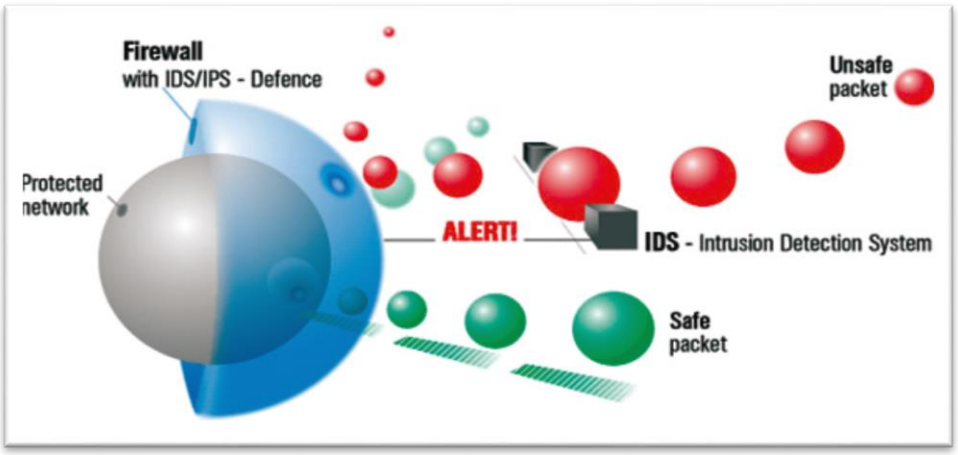
- Anti pop-Ups. Tiene como finalidad impedir que se ejecuten las ventanas pop-ups o emergentes, es decir a aquellas ventanas que surgen repentinamente sin que el usuario lo haya decidido, mientras navega por Internet.

- Anti-Spam. Se denomina spam a los mensajes basura, no deseados o que son enviados desde una dirección desconocida por el usuario"[81].

[81] Ibídem.

7.8 IDS

Figura. 9. Esquema de un IDS elemental



Fuente: http://www.trendcorp.com.pe/img/dummies/intruso.jpg

El término IDS (Sistema de detección de intrusiones) “hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión”[82].

Según Mira[83] los IDS o sistema de detector de intrusos “son equipos que permiten por medio de patrones y comportamientos de conexiones o tipos de ataques de red limitar el acceso o evitar las intrusiones a los sistemas”.

> “Los IDS permiten igualmente monitorear las diferentes técnicas de instrucción de red e interactuar con el firewall y bloquear el acceso, el firewall que tienen internamente ayuda a eliminar las conexiones que son activadas por medio de una vulnerabilidad o un escaneo de red que pueda exponer información de los equipos y redes de una compañía”[84].

[82] Op. Cit. CCM. 2015.
[83] MIRA ALFARO, Emilio José. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. {En línea}. {24 de Marzo de 2015}. Disponible en: (http://rediris.es/cert/doc/pdf/ids-uv.pdf).
[84] Ibídem.

A diferencia del firewall, los IDS son equipos proactivos y son configurados para que eliminen el riesgo antes de que se active o sea efectivo, estos riesgo van desde accesos a redes o equipos hasta la explotación de fallos en aplicaciones o software que estén instalados en los equipos de cómputo o servidores de aplicaciones.

Igualmente los IDS se configuran para generar alertas proactivas y activas, los registros o LOG determinan los comportamientos de los sistemas y posibles intrusiones, esto apoya al administrador de seguridad para mejorar la configuración y proteger los sistemas.

Según CCM se puede hablar de dos familias importantes de IDS, las cuales son:

"- El grupo N-IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red.

- El grupo H-IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host".

> "Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro"[85].

CCM considera que el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura

[85] CCM (2015) Sistema de detección de intrusiones (IDS) Disponible en: http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer).[86]

7.8.1 Topologías de IDS. Montañana[87] menciona las muchas formas de añadir "las herramientas IDS a nuestra red". Para el autor *"cada una de ellas tiene su ventaja y su desventaja. La mejor opción debería ser un compendio entre coste económico y propiedades deseadas, manteniendo un alto nivel de ventajas y un número controlado de desventajas, todo ello de acuerdo con las necesidades de la organización"*[88].

> *"Por este motivo, las posiciones de los IDS dentro de una red son varias y aportan diferentes características. A continuación vamos a ver diferentes posibilidades en una misma red. Imaginemos que tenemos una red dónde un cortafuegos nos divide la Internet de la zona desmilitarizada (DMZ – Demilitarized Zone), y otro que divide la DMZ de la intranet de la organización como se muestra en la Fig. 9. Por zona desmilitarizada entendemos la zona que debemos mostrar al exterior, la zona desde la cual mostramos nuestros servicios o productos"*[89].

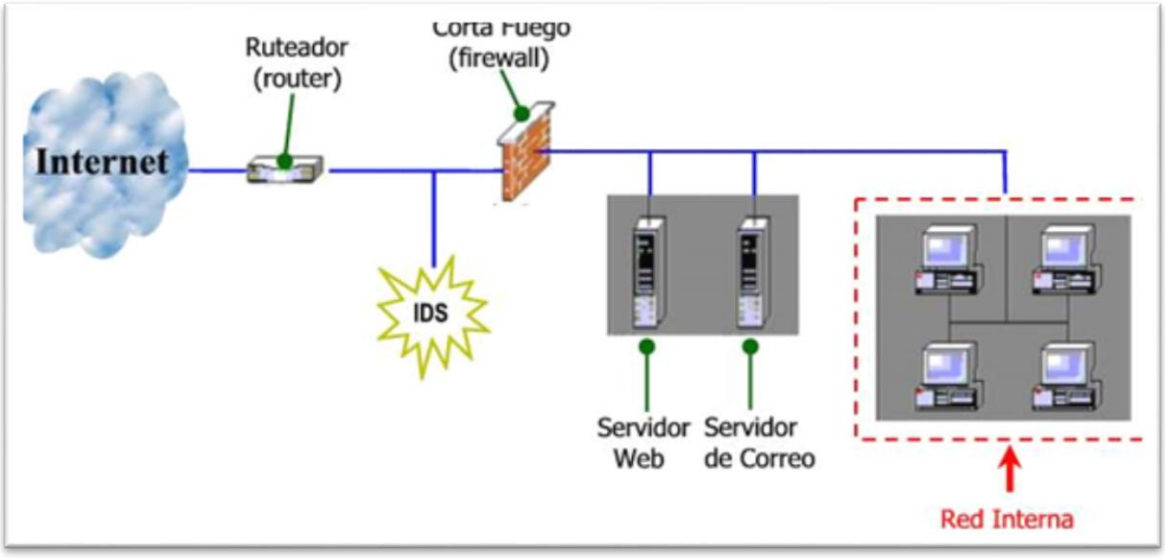
[86] CYRILLE, Larrieu. Sistema de Detección de Intrusiones. {En línea}. {3 de Agosto de 2015}. Disponible en: (http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids).

[87] MONTAÑANA, Rogelio (2013) Sistemas de Detección de Intrusiones (IDS). Universidad de Valencia Disponible en: www.uv.es/~montanan/redes/trabajos/IDSs.doc

[88] Ibídem.

[89] Ibídem.

Figura 10. Red con IDS simple



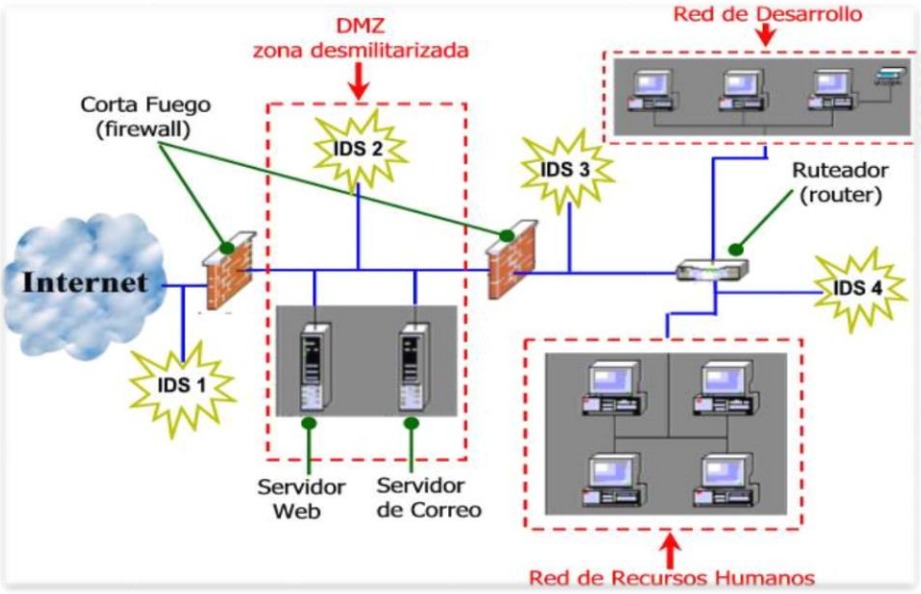
Fuente: www.uv.es/~montanan/redes/trabajos/IDSs.doc

> "Si situamos un IDS antes del cortafuegos exterior permitiría detectar el rastreo de puertos de reconocimiento que señala el comienzo de una actividad hacking, y obtendríamos como ventaja un aviso prematuro. Sin embargo, si los rastreos no son seguidos por un ataque real, se generará un numeroso número de alertas innecesarias con el peligro de comenzar a ignorarlas"[90].
> *"Si optamos por colocar el IDS en la zona desmilitarizada (DMZ) tendríamos como ventaja la posibilidad de adecuar la base de datos de atacantes del NIDS para considerar aquellos ataques dirigidos a los sistemas que están en la DMZ (servidor web y servidor de correo) y configurar el cortafuegos para bloquear ese tráfico. Así mismo, un NIDS dentro de la red, por ejemplo, de Recursos Humanos podría monitorear todo el tráfico para fuera y dentro de esa red. Este NIDS no debería ser tan poderoso como los comentados anteriormente, puesto que el volumen y el tipo de tráfico es más reducido"*[91].

El resultado lo podemos visualizar en la Figura 10.

[90] Ibídem.
[91] Ibídem.

Figura 11. Red completa con IDS



Fuente: www.uv.es/~montanan/redes/trabajos/IDSs.doc

> *"El IDS1 se encargaría de avisar del rastreo de puertos, y si es reactivo podría enviar un "aviso" tanto al que está rastreando (por ejemplo un ping a la dirección que emite el paquete) como al encargado de la seguridad de la organización. El IDS2 se encargaría de vigilar la zona desmilitarizada y analizar el tráfico que reciben tanto el servidor web como el servidor de correo. Los otros dos IDS se encargarían de la red interna, el IDS3 de la totalidad de la red, y el IDS4 de una subred, en este caso la de RRHH. Estos dos NIDS internos (el IDS3 y el IDS4) podrían ser sensores que recogiesen la información y lo enviasen a una consola dónde se realizarían los cálculos".*[92]

7.8.2 Función de los IDS. La integridad de un sistema "se puede corromper de varias formas y la forma de evitar esto es con la instalación de Sistemas de Detección de Intrusos en Tiempo Real"[93], quienes:

[92] MONTANAN, Rogelio. Redes, trabajos IDS. {En línea}. {18 de Junio de 2015}. Disponible en: (www.uv.es/~montanan/redes/trabajos/IDSs.doc).

[93] Op. Cit. Segu.info. 2014.

- Inspeccionan el tráfico de la red buscando posibles ataques.

- Controlan el registro de los servidores para detectar acciones sospechosas (tanto de intrusos como de usuarios autorizados).

- Mantienen una base de datos con el estado exacto de cada uno de los archivos (Integrity Check) del sistema para detectar la modificación de los mismos.

- Controlan el ingreso de cada nuevo archivo al sistema para detectar Caballos de Troya o semejantes.

- Controlan el núcleo del Sistema Operativo para detectar posibles infiltraciones en él, con el fin de controlar los recursos y acciones del mismo.

- Cada una de estas herramientas permite mantener alejados a la gran mayoría de los intrusos normales.[94]

7.8.3 Características de los IDS. Según info[95] todo sistema de detección de intrusos debería, sea cual sea el mecanismo en que esté basado, contar con las siguientes características:

"- Funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en background dentro del equipo que está siendo observado. Sin embargo, no debe ser una "caja negra" (debe ser examinable desde el exterior).

- Ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.

En relación con el punto anterior, debe ser resistente a perturbaciones. El sistema puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.

[94] ARDITA, Julio César. Protección. {En línea}. {5 de Abril de 2015}. Disponible en: (https://www.segu-info.com.ar).
[95] Op. Cit. Segu.info. 2014.

- Debe ser fácilmente adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.

- Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo"[96].

7.8.4 Fortalezas de IDS

- Poder de reacción para prevenir el daño.

- Es una herramienta útil como arma de seguridad de la red.

- Ayuda a identificar de dónde provienen los ataques que se sufren.

- Recoge evidencias que pueden ser usadas para identificar intrusos.

- Funciona como "disuasor de intrusos".

- Es una parte de la infraestructura para la estrategia global de defensa.

- La posibilidad de detectar intrusiones desconocidas e imprevistas. Pueden incluso contribuir (parcialmente) al descubrimiento automático de esos nuevos ataques.

- Son menos dependientes de los mecanismos específicos de cada sistema operativo.

- Pueden ayudar a detectar ataques del tipo "abuso de privilegios" que no implica realmente ninguna vulnerabilidad de seguridad. En pocas palabras, se trata de una aproximación a la paranoia: "todo aquello que no se ha visto previamente es peligroso".

- Menor costo de implementación y mantenimiento al ubicarse en puntos estratégicos de la red.

- Dificulta el trabajo del intruso de eliminar sus huellas.

[96] Ibídem.

7.8.5 Debilidades de IDS.

"- No existe un parche para la mayoría de bugs de seguridad.

- Se producen falsas alarmas.

- No es sustituto para un buen Firewall, una auditoría de seguridad regular y una fuerte y estricta política de seguridad."[97]

7.8.6 Inconvenientes de IDS

- La alta tasa de falsas alarmas dado que no es posible cubrir todo el ámbito del comportamiento de un sistema de información durante la fase de aprendizaje.

- El comportamiento puede cambiar con el tiempo, haciendo necesario un re-entrenamiento periódico del perfil, lo que da lugar a la no disponibilidad del sistema o la generación de falsas alarmas adicionales.

- El sistema puede sufrir ataques durante la fase de aprendizaje, con lo que el perfil de comportamiento contendrá un comportamiento intrusivo el cual no será considerado anómalo.[98]

7.9 CONTRASEÑAS

Astorga facilita ciertos preceptos clave para la formulación contraseñas, destinadas a aumentar la seguridad. Dentro de estas se encuentran:

> *"- Deshabilitar el almacenamiento de Hash Lan Manager: Windows, por compatibilidad con versiones anteriores del sistema operativo, almacena las contraseñas en dos formatos, en LAN Manager y NTLM, el primero es por demás inseguro*[99]*.*

[97] Ibídem.
[98] Ibídem.
[99] Op. Cit. Astorga. 2013.

- Relacionado con el punto anterior, es recomendable forzar la autenticación a que sólo sea mediante NTLM.

- Mantener un historial de contraseñas de por lo menos las seis últimas; así, cuando un usuario sea forzado a cambiar su contraseña, no podrá repetirla.

- La edad máxima de las contraseñas dependerá del negocio y del usuario, pero no es recomendable utilizar contraseñas "eternas" por el riesgo que ello implica.

- El tamaño de la contraseña y la forma en que la misma deba construirse es muy importante, un número mínimo de ocho caracteres es recomendable, así como utilizar letras mayúsculas, minúsculas, números y signos especiales.

- Es recomendable bloquear las cuentas tras un cierto número de intentos fallidos, es importante recalcar que en este punto deberemos tener especial cuidado, ya que si bien nos protege contra ataques de diccionario, también nos puede llevar a un ataque de DoS.

- Un punto importante es el evitar que sea mostrado el último usuario que se firmó al equipo, de esta forma no le estamos regalando a un posible intruso uno de los datos de entrada al equipo.

- Debido al punto anterior es aconsejable renombrar la cuenta de administrador.

- Activar el protector de pantalla protegido por contraseña y con un tiempo corto de activación es útil para evitar que por algún descuido se deje una sesión activa".[100]

[100] Ibídem.

7.10 CRIPTOGRAFÍA

Figura 12. Inicios de la Criptografía.

Fuente: https://it-skull.com/images/headers/Skytale_Fotor.jpg

Es un conjunto de técnicas utilizadas para modificar información, de tal manera que se vuelva incomprensible para receptores no autorizados. Es decir, “permite enviar y recibir datos en un formato ininteligible para un tercero; accesibles únicamente si se dispone de una llave de acceso o contraseña de desbloqueo. La criptografía permite enviar información segura sobre un canal inseguro”[101].

Todas estas técnicas tienen base en el campo de las matemáticas e informática a través de algoritmos o protocolos.

SSH: “Este paquete de software permite las conexiones remotas y otras funciones (transferencia de archivos, por ejemplo), al igual que lo hace telnet pero codificando la información que se transmite por la red y ofreciendo un método de autentificación de los extremos de la comunicación. El hecho de que la información viaje codificada

[101] FEBLES RODRÍGUEZ, Juan Pedro. Criptografía y Redes. {En línea}. {1 de Agosto de 2015}. Disponible en: (http://maestriainformaticamg.blogspot.com.co/2012/07/presentacion-tema-5.html).

a través de la red hace que los datos capturados por un posible sniffer no puedan ser utilizados por un atacante."[102]

Existen varias formar de cifrar la información, entre estas esta el cifrado por contraseña que lo que se practica es cifrar el contenido y por medio de una contraseña asignada se aplica el algoritmo el cual con base a esta cifra la información. El cifrado con llaves es una técnica mucho más segura ya que por medio de una llave pública y una privada se realiza en cifrado, lo interesante de este cifrado es que si no se tiene la llave publica ya la contraseña no es posible descifrar el contenido siendo así más seguro y menos riesgo de ser vulnerable a técnicas de fuerza bruta.

El concepto de cifrado se aplica tanto en archivos como bases de datos, en la actualidad existe varias herramientas que cifran información que practican este tipo de cifrados entre ellas podemos mencionar el PGP que es un software de pago y utiliza las dos técnicas y GPG que comparte los dos conceptos pero es de libre distribución.

El cifrado es una forma efectiva de mitigar el concepto ataque en profundidad ya que si por medio de una vulnerabilidad o virus informático el atacante tiene acceso al sistema no podrá contar con la suerte de tener la información disponible legiblemente, esto hará que la información cuente con seguridad e integridad.[103]

[102] UNTIVEROS, Sergio. Sniffing. {En línea}. {27 de Junio de 2015}. Disponible en: (http://www.aprendaredes.com).

[103] JIMENEZ SOTO, León Manuel. Redes de Área Local: Sniffers o Analizadores de Paquetes. {En línea}. {27 de Agosto de 2015}. Disponible en: (https://infosegur.wordpress.com/category/4-criptografia/).

7.11 USOS DE SNIFFER (ANALIZADOR DE PAQUETES)

Un Sniffer es un programa de captura de las tramas de una red de computadoras. Dentro de los usos y empleos inherentes a los analizadores de paquetes se cuentan el monitoreo de redes con el fin de identificar y analizar fallas o bien para efectuar ingeniería en protocolos de red. *"También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc."*[104]

Los analizadores de paquete o Sniffers son programas que apoyan al oficial de seguridad a analizar el tráfico de red que está activo, este puede determinar ataques informáticos en una red corporativa. Los sniffers pueden detectar si una dirección IP intenta vulnerar un servidor o equipos que estén en la red, estos se puede configurar con reglas para filtrar determinados paquetes e identificar qué tipo de técnica se utiliza para ser intrusivo.

Las técnicas que puede identificar un sniffer entre otras son DNSSPOFING, IPSPOFING y ARPSPOFING, el DNSSPOFING vulnera los servidores DNS para redirigir el trafico http a otro servidor web y capturar credenciales por ejemplo, el IPSPOFING asigna una dirección IP de la red que ya fue asignada para hacerse pasar por el equipo que la tenía asignada y el ARPSPOFING asigna la dirección física o MAC de un equipo que ya la tenía para suplantarlo, estas técnicas pueden pasar por alto el firewall o antivirus y es posible detectarlos con un sniffer.[105]

---

[104] CEQUEDA, Jean Polo (2012) Robo de información mediante la interceptación de mensajes. Disponible en: https://seguridadinformaticaufps.wikispaces.com/ROBO+DE+INFORMACI%C3%93N+MEDIANTE+LA+INTERCEPTACI%C3%93N+DE+MENSAJES

[105] COLASOFT (2014) What They Are and How to Protect Yourself. Disponible en: http://www.colasoft.com/resources/sniffer.php

7.11.1 Utilidad.

Los principales usos que se le pueden dar, según Facundo Gallo[106], son:

> *"- Captura automática de contraseñas enviadas en claro y nombres de usuario de la red. Esta capacidad es utilizada en muchas ocasiones por crackers para atacar sistemas a posteriori.*
>
> *- Conversión del tráfico de red en un formato inteligible por los humanos.*
>
> *- Análisis de fallos para descubrir problemas en la red, tales como: ¿por qué el ordenador A no puede establecer una comunicación con el ordenador B?*
>
> *- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.*
>
> *- Detección de intrusos, con el fin de descubrir hackers. Aunque para ello existen programas específicos llamados IDS (Intrusion Detection System, Sistema de Detección de intrusos), estos son prácticamente analizadores con funcionalidades específicas.*
>
> *- Creación de registros de red, de modo que los hackers no puedan detectar que están siendo investigados.*
>
> *- Para los desarrolladores, en aplicaciones cliente-servidor. Les permite analizar la información real que se transmite por la red".*[107]

7.11.2 Medidas a tomar. Untiveros[108] resalta la necesidad de crear sockets raw, en el que el intruso sea raíz, en modo promiscuo.

En primer lugar, se aconseja el uso de una topología en estrella con concentradores inteligentes, pues es una configuración más apropiada para evitar la instalación de sniffers. Otra medida frente a los sniffers en modo promiscuo "*es instalar*

---

[106] GALLO, Facundo (s.f.) Inseguridad informática. Disponible en: http://bit.ly/1W2YaxJ

[107] Ibídem.

[108] UNTIVEROS, Sergio (s.f.) Aprende a mirar dentro de la red con un "Sniffer". Disponible en: www.aprendaredes.com/dev/articulos/aprende-a-mirar-dentro-de-la-red-con-un-sniffer.htm

adaptadores de red que no permitan ser configurados en este modo, ya que existen este tipo de dispositivos"[109].

> *"Si el sniffer no se ha ocultado convenientemente, las herramientas de monitorización mostrarán el proceso que se está ejecutando, el fichero donde se están grabando los datos y la conexión de red*"[110]*.*

Una medida bastante drástica consiste en recompilar el kernel de forma que no ofrezca soporte para poner los adaptadores de red en modo promiscuo. Es una solución drástica, al igual que la adquisición de una tarjeta de red que no soporte este modo.

7.12 POLÍTICAS DE SEGURIDAD

Poyato et al.[111] Establece que muchas organizaciones *"no tienen establecida una política de seguridad en la que se indiquen los derechos y obligaciones, o las sanciones en las que pueden incurrir los usuarios"*. En este sentido, formula las siguientes políticas que permiten blindar en seguridad a los sistemas:

7.12.1 Políticas de passwords y cuentas. El administrador de la red debe establecer unas políticas de passwords en la que se especifique:

> "- Una duración máxima de la contraseña (aconsejable unos 90 días).
>
> - Una longitud mínima (aconsejable un mínimo de 8 caracteres).
>
> - Un histórico de la contraseña (unas 5 contraseñas).
>
> - Un bloqueo automático tras sucesivos fallos de login (unos 5 fallos)"[112].

[109] Ibídem.
[110] Ibídem.
[111] Poyato et al. (2000) Recomendaciones de seguridad. Disponible en: https://www.fi.upm.es/docs/servicios/seguridad_informatica/371_recomendaciones.pdf
[112] Ibídem.

7.12.2 Políticas generales de seguridad.

Una política de seguridad informática "es una forma de comunicarse con los usuarios y los gerentes"[113].

De acuerdo con Poyato et al., se deben establecer canales formales y eficaces que interconecten la actuación del talento humano, en función de recursos y servicios informáticos. "No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el porqué de ello. Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía"[114].

- Elementos de una política de seguridad informática.

"*Una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante"*[115].

Las PSI, según Poyato et al., deben considerar entre otros, los siguientes elementos:

> "- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

[113] UNTIVEROS, Sergio (s.f.) Politicas, Planes y Procedimientos de Seguridad. Disponible en: https://seguridadinformaticaufps.wikispaces.com/Politicas,+Planes+y+Procedimientos+de+Seguridad
[114] Ibídem.
[115] Ibídem.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

- Definición de violaciones y de las consecuencias del no cumplimiento de la política.

- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

- Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios".

Los autores consideran que las PSI determinan las posibilidades de una compañía en función de su seguridad. A partir de estas se concretan las acciones que permiten llevar a cabo las tareas de la empresa.

"Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa"[116].

7.12.3 Algunos parámetros para establecer políticas de seguridad.

"Si bien las características de las PSI que hemos mencionado hasta el momento, nos muestran una perspectiva de las implicaciones en la formulación de estas directrices, revisaremos a continuación, algunos aspectos generales recomendados para la formulación de las mismas. Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.

- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

[116] Ibídem.

- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

Un último consejo: no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas.

- Política de privacidad. Determina las expectativas razonables de privacidad sobre temas relacionados con monitoreo de correos electrónicos, acceso a archivos y registro de teclados. Podría incluir también políticas acerca de registro, escucha y control de llamadas telefónicas, control de accesos a sitios web, uso de herramientas de mensajería instantánea, etc.

- Política de acceso. Define derechos o privilegios de acceso a activos o recursos de información protegidos. Especifica comportamientos aceptables para usuarios, empleados soporte y directivos. Debe incluir reglas respecto a las conexiones y accesos externos, así como reglas acerca de la comunicación de datos, conexiones de dispositivos a las redes e inclusión de nuevas aplicaciones informáticas en los sistemas existentes

- Política de responsabilidad. Define las responsabilidades de usuarios, personal de mantenimiento y directivos. Debe especificar la capacidad de realizar auditorías y sus características, y proveer las guías para el registro y manejo de incidentes de seguridad.

- Política de autenticación. Debe establecer los mecanismos de "confianza" mediante el uso de una política de contraseñas apropiadas. Debe considerar, si aplica, políticas de autenticación local y de acceso remoto.

- Política de mantenimiento de los sistemas relacionados con la tecnología de la información. Describe cómo deberá hacerse el mantenimiento realizado tanto por personal interno como externo a la organización. Debe establecerse si se admite o no algún tipo de mantenimiento remoto (por ejemplo, por internet o por módem), y las reglas que aplican, así como los mecanismos internos de control".[117]

[117] ROBAYO, Javier. Políticas de seguridad. {En línea}. {12 de Junio de 2015}. Disponible en: http://jhrlsegredes.blogspot.com/

8. DESCRIPCIÓN DE LA EMPRESA SITIOSDIMA.NET

8.1 DESCRIPCIÓN GENERAL

Sitiosdima.net es una empresa proveedora de servicios de internet donde sus plataformas soportan portales y sitios web de alto tráfico, entre sus servicios ofrece hosting, registro de dominios, desarrollo de software web, diseño gráfico y publicidad de en la red.

Cuenta con talento humano capacitado para la gestión y administración de las plataformas las cuales esta conformadas de 5 servidores dedicados con sistemas operativo Linux y 10 computadores para la gestión administrativa del negocio y soporte para los clientes.

Dicha empresa cuenta con procesos de administración remota a los sistemas de hospedaje de los diferentes clientes, estos procesos se realizan desde equipos con sistemas operativos Windows y se ejecutan desde una terminal SSH bajo la conexión de una VPN, este proceso a nivel de redes está asegurado y con un grado alto de confiabilidad. El proceso de administración remota puede ser debilitado en el momento que el sistema operativo sea infectado o manipulado por software malicioso, el cual puede llegar a ser instalado en el sistema mediante una vulnerabilidad del sistema operativo, fallas de configuración de seguridad interna o manipulación del usuario administrador.

Dado lo anterior, surge la necesidad de analizar y plantear las medidas requeridas tendientes a fortalecer y configurar apropiadamente los sistemas operativos de la organización, para tal efecto se estará implementando estrategias de seguridad basadas en la información recabada en la presente monografía.

8.2 PERSONAL DE LA EMPRESA

Los empleados que trabajan por prestación de servicios se encuentran en la capacidad de liderar, administrar y gestionar los servidores dedicados que permiten tener los sitios en un alto grado de disponibilidad, para ello la empresa debe tener los siguientes perfiles actualmente:

8.2.1 Personal administrativo.

- Gerencia: El gerente se encarga de gestionar los procesos de innovación y continuidad del negocio, al igual que su funcionamiento y cumplimiento de la misión y visión de la empresa.

- Apoyo administrativo: Apoya los procesos de gestión documental y servicios de contabilidad.

8.2.2 Personal de ingeniería.

- Ingenieros de nivel: Los ingenieros de primer nivel apoyan el soporte técnico a los usuarios para dar soluciones inmediatas a problema que no tengan gestión directa con los servidores.

- Ingenieros de segundo nivel: El segundo nivel hace referencia a solucionar problemas más afondo del usuario, estos problemas hacen más referencia a la administración de los servidores y manipulación del mismo.

8.2.3 Personal de ventas-

- Comerciales: Los ingenieros comerciales apoyan los procesos de ventas y contratación de servicios.

8.3 MISIÓN

Impulsar las pequeñas y medianas empresas, usando estrategias comerciales de potencias mundiales por medio del diseño Web y publicidad constante digital, creando un trabajo de excelente calidad que satisfaga al cliente y genere reconocimiento ante sus consumidores.

8.4 VISIÓN

Ser reconocidos a nivel nacional como una empresa de alta calidad y generadora de servicios de primera clase, frente a otras empresas de servicios de internet. Siempre pensando en satisfacer las necesidades del usuario, teniendo presente que el cliente es la razón de ser de la empresa sitiosdima.net.

9. DISEÑO METODOLÓGICO PRELIMINAR A IMPLEMENTAR EN PRUEBAS

La implementación de un sistema de aseguramiento en sistemas operativos, parte del concepto de defensa en profundidad donde el objetivo es proteger un sistema en capas para evitar una intrusión en su aspecto más intrusivo, para ello se pretende fortalecer configuraciones y estados de software y aplicaciones que están instaladas en dicho sistemas operativos.

Como fases de implementación se encuentran:

- Recolección de información

- Análisis de los sistemas operativos

- Configuración segura y aplicación de ServicePacks y Hotfixes

- Análisis y configuración de políticas de seguridad de usuarios, archivos y registros del sistema.

- Análisis de resultados

9.1 PROCEDIMIENTOS DE ASEGURAMIENTO

9.1.1Hardening Windows.

- Recolección de la información.
- Análisis de riesgos.
- Análisis de vulnerabilidades.
- Fallos identificados
- Editor de Registros de Windows

9.1.2 Vulnerabilidades.

- Acciones de seguridad en sistema operativo
- Procesos de aseguramiento
- Verificación de actualizaciones
- Análisis de configuración por defecto
- Seguridad básica aplicada
- Efectos influyentes por mala configuración

9.1.3 Aplicación de aseguramiento.

- Actualizaciones de seguridad
- Políticas de seguridad
- Configuración de permisos de usuario y aplicaciones
- Aseguramiento de configuraciones por defecto
- Permisos de archivos y entradas del Registro

9.1.4 Resultados De Aseguramiento (Informes).

- Informe de resultados y estado de seguridad del aseguramiento
- Aseguramiento de la información
- Políticas de seguridad de la información
- Aplicación de políticas de seguridad
- Acceso de usuario y contraseña
- Actualizaciones y registros de log
- Gestión del riesgo
- Asignación de acceso a los sistemas de información
- Atención a incidentes
- Gestión de la seguridad informática de la empresa
- Revisión estructurada del plan

- Prueba de la lista de verificación
- Simulaciones
- Prueba en paralelo
- Prueba de interrupción completa

9.2 PERSONAL REQUERIDO PARA REALIZAR LAS PRUEBAS

- Ingenieros de Sistemas con Especialización en Seguridad Informática e Ingeniero de las Telecomunicaciones, Especialista en pedagogía de la Virtualidad.

- Integrantes del área de contratación

- Alta gerencia y planeación

- Personal en el área de información.

10. RECURSOS A IMPLEMENTAR EN PRUEBAS

10.1 RECURSOS MATERIALES

En el área de recursos materiales a implementar en las pruebas estimadas, es susceptible de elección según los recursos disponibles. Sin embargo, a continuación se deja en consideración la descripción de un equipo de computación el cual se considera básico en la realización de las pruebas planteadas. De igual manera se describe el tipo de conexión a la red y las herramientas, llámese Software ideales en la ejecución de las pruebas, recalcando que no es camisa de fuerza su uso según lo aquí señalado, pues como bien es sabido tanto el Hardware como el Software experimentan cambios exponenciales cada día.

Tabla 1. Hardware y Software a implementar en pruebas.

HARDWARE	
Ítem	**Cantidad/Descripción**
Equipo de computación	
Computador portátil	1
Costo por equipo	$2800.000
Características	- Intel Core i7-4710HQ Processor Frecuencia 2.5 GHz a 3.5 Ghz con Turbo Boost 2.0, 4 Núcleos totales, 8 HILOS DE PROCESAMIENTO), 6MB en Cache, este procesador viene con Turbo Boost 2.0 - Sistema operativo WINDOWS 8.1 SL A 64 BITS. - Memoria RAM 8 Gb (Expandible a 16Gb). - Discos Duro de 1000 Gb (5400 RPM) - Pantalla de 15.6" Pulgadas retroiluminada LED - ANTIREFLEJO Resolución 1920 x 1080 FHD - Motor Gráfico Nvidia GTX 860M CON 4 GB DE VIDEO DEDICADO GDDR5 (Ancho de Banda 80Gb/s) - BLUETOOTH 4.0 original en Motherboard 1 Puerto HDMI exporta video a una definición de 1080p 1 RANURA LECTORA DE TARJETAS SD

	3 Puertos USB 3.0
Usabilidad	Escaneo de equipos en la red y generador de reportes.
Conexiones inalámbricas	
Antenas Wifi	1
Características	Antena Wifi Usb 68dbi Kasens Ks1680
Costo por unidad	$120.000
Usabilidad	Escaneo de equipos desde redes inalámbricas.
Dispositivos USB	
USB	2
Costo por unidad	$32.000
Usabilidad	Almacenamiento de log y registros de escaneo
SOFTWARE	
Sistema operativo Linux	
Cantidad	1
Versión	KALI LINUX
Módulo de aplicación	METAEXPLOIT, NEXUS
Costo	Software libre
Usabilidad	Escaneo y detención de vulnerabilidades en los sistemas operativos.

Fuente: Los autores.

10.2 RECURSOS INSTITUCIONALES

La razón que motiva a continuar trabajando el proceso de concientización en cuanto al proceso de la seguridad informática en las organizaciones, los administradores de un centro de datos, de red y en general todo aquel encargado de la seguridad de los equipos de cómputo debe tener una guía que le oriente para comenzar a robustecer la seguridad de los sistemas operativos en cuanto el software sea “sacado del empaque” tomando siempre en cuenta que el robustecimiento del mismo es en función de las actividades que realizará y el entorno al que pertenece el equipo.

El problema destaca por la falta de recursos técnicos de los administradores de un centro de datos con respecto a la información necesaria para realizar le selección y robustecimiento de los sistemas operativos en servidores, lo cual conlleva a tener deficiencias en la instalación y configuración de la seguridad en el sistema operativo.

10.3 RECURSOS FINANCIEROS

Colciencias, con el apoyo del Banco Interamericano de Desarrollo (BID), presentó el programa Finbatec -Fomento a la Inversión en Empresas de Base Tecnológica e Innovadoras- a través del cual se respaldará a los empresarios para encontrar financiación para sus proyectos, a través de los fondos de inversión e inversionistas en capital. Inicialmente estará en las seis ciudades.

Según lo explicó Colciencias, en los países avanzados los fondos de inversión en capital como socios de las empresas, sirven para financiar y para agregar valor y proyectar desde una idea y su validación técnica y comercial, pasando a apoyar la transición de crecimiento y expansión propios de las mipymes en las distintas etapas de desarrollo, hasta ayudar a consolidar grandes empresas. Finbatec ayudará en la solución de las necesidades de financiación, dependiendo de la magnitud del proyecto.

10.5 PRESUPUESTO PARA LA REALIZACIÓN DE PRUEBAS EN LA EMPRESA SITIOSDIMA.NET

10.5.1 Software. Para la realización de las pruebas en la empresa sitiosdima.net, se requiere software que prometa alcances de recolección de información, evaluación y escaneo de vulnerabilidades en los sistemas operativos Windows, por lo cual será utilizado diferentes aplicaciones que son de carácter libre y no se requiere licencia para la instalación y configuración del mismo.

Para el ajuste de los resultados igualmente las herramientas generan reportes y no es necesario adquirir otros programas.

10.5.2 gastos operativos. La ejecución de un proyecto cualquiera que éste sea, implica una serie de gastos de operación, insumos y desde luego de mano de obra. Con es de suponer, los gastos de ejecución son una variante relativa en tiempo y dimensión del proyecto, teniendo presente esta premisa, en la Tabla 3, se hace un breve estimativo en cifras calculadas de los gastos que conllevan la realización de las pruebas planteadas, cifras generadas a la fecha de redacción del presente documento.

Tabla 2. Costos de ejecución.

Internet	**Mifi conexión internet 4G 3 meses.**	**$300.000**
Gastos de ejecución	Transporte 3 meses	$600.000
Gasto de comunicaciones	Telefonía celular 3 meses	$210.000
TOTAL		$1.110.000
HARDWARE		$2.980.000
GASTOS OPERATIVOS		$1.110.000
TOTAL DE GASTOS		$4.090.000

Fuente: los autores.

10.6 AUTORES Y COLABORADORES EN LA CRECIÓN Y DESARROLLO DE LA MONOGRAFÍA

DIRECTOR. Rafael Pérez Holguín, nacido y criado en Sogamoso – Boyacá, Ingeniero de Sistemas, próximo a grado como Ingeniero de las Telecomunicaciones, Con "Especialización en pedagogía de la Virtualidad", "Master en dirección Estratégica en tecnologías de la Información, candidato al doctorado en Proyectos de la UNINI de México. Pertenece a la Escuela de Ciencias Básicas Tecnológicas e Ingeniería – ECBTI como Tutor de Tiempo Completo de la Zona: Amazonía Orinoquia, CEAD Yopal - Casanare.

Javier Humberto Robayo López, nacido en Carmen de Carupa – Cundinamarca el 18 de Julio de 1972. Se graduó en el Instituto Cultural de Villavicencio – Meta y es egresado de la Universidad Nacional Abierta y a Distancia como Ingeniero de Sistemas. Actualmente estudiante en la misma Universidad en Especialización en Seguridad Informática. Sus áreas de interés incluyen, entre otras, las TCs y la Tecnología.

Richar Mauricio Rodríguez, nacido en Bogotá en el año de 1974, ingeniero de sistemas de la Universidad Nacional Abierta y a Distancia, laboro en la Fiscalía General de la Nación y actualmente asesor a empresas en sistemas de información y seguridad informática.

CONCLUSIONES

- Se conoció el método hardening y las actividades que deben realizarse en la aplicación del proceso de aseguramiento del sistema para lograr un estado ideal de protección.

- Se estudió las implicaciones que tiene la aplicación del hardening en la instalación de un sistema operativo Windows, especialmente al deshabilitar servicios instalados por defecto.

- Se logró detallar gráfica y conceptualmente en que consiste el concepto de defensa en profundidad, el proceso de protección estructurado y niveles de seguridad frente a cualquier fenómeno de amenaza.

- Se indagó a cerca de las herramientas implementadas en la exploración de puertos de un sistema operativo, sus características, bondades y modos de uso, algunas aplicaciones estudiadas fueron, CurrPorts y Simple Port Tester.

- Se identificó el papel que desempeña un Firewall en la seguridad de un sistema operativo, tras la debida configuración, restringir conexiones externas a servicios y puertos del equipo hacen de ésta una aplicación esencial en el Hardening de un sistema.

- Se relacionó el vínculo que tienen aplicaciones como los IDS, Sniffers, Antivirus en materia de seguridad, sus características de aplicación, estructura, fortalezas, debilidades e inconvenientes.

- Se analizó la implementación de políticas de seguridad y la importancia que tiene capacitar al personal de la organización para interpretar de manera exitosa los planteamientos entre usuarios y gerencia.

RECOMENDACIONES

Realizar las configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de máquina un sistema operativo, no es una tarea fácil y requiere tomar conciencia de seguir estrictamente las políticas de seguridad planteadas.

Implementar actividades como el upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, entre otras medidas para evitar cualquier entrada de malware desde un medio de almacenamiento externo es una medida de inaplazable implementación.

Se debe realizar la instalación segura del sistema operativo, conocido como instalación mínima, evitando la instalación de componentes que se consideran innecesarios y que pueden convertirse en un factor de riesgo o vulnerabilidad.

Existe gran cantidad de herramientas como CurrPorts, Simple Port Tester, Zenmap, Antivirus entre otras, que sirven de apoyo en la implementación de estrategias tipo Hardening de las cuales es necesario conocer sus características y de ésta manera lograr hacer mejor uso de éstas.

La instalación, configuración y actualización de programas de seguridad tales como Antivirus, Antispyware, firewall y similares son de vital importancia en busca del robustecimiento del sistema.

REFERENCIAS BIBLIOGRÁFICAS

ACOSTA, David. Estandares de Configuración Segura Hardening en pci. {En línea}. {09 de Marzo de 2015}. Disponible en: (http://www.pcihispano.com/estandares-de-configuracion-segura-hardening-en-pci-dss/).

ADMIN. Historia de la criptografía. {En línea}. {18 de Febrero de 2015}. Disponible en: (https://it-skull.com/images/headers/Skytale_Fotor.jpg).

ADMIN. Medidas de seguridad básica: Los puertos de tu router. {En línea}. {12 de Marzo de 2015}. Disponible en: (http://www.fundacionctic.org/sat/articulo-medidas-de-seguridad-basicas-los-puertos-de-tu-router).

ADMIN. Mejorar Seguridad de Windows cerrando puertos abiertos. {En línea}. {3 de Abril de 2015}. Disponible en: (http://www.osflash.com/mejorar-seguridad-de-windows-cerrando-puertos-abiertos/).

ADMIN. Qué son los virus informáticos. {En línea}. {06 de Febrero de 2015}. Disponible en: (http://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1.do).

ALFON. Breve introducción a los sistemas IDS y Snort. {En línea}. {22 de Marzo de 2015}. Disponible en: (http://www.maestrosdelweb.com/snort/).

ARDITA, Julio César. Protección. {En línea}. {5 de Abril de 2015}. Disponible en: (https://www.segu-info.com.ar).

ASTORGA, Agustín. Hardening de un sistema MS Windows. {En línea}. {9 de Enero de 2015}. Disponible en: (http://esemanal.mx/2006/11/hardening_de_un_sistema_ms_windows/).

B1NARY0. Cierre de Puertos Abiertos. {En línea}. {2 de Mayo de 2015}. Disponible en: (http://www.b1nary0.com.ar).

BEAL, Vangie. Firewall. {En línea}. {17 de Enero de 2015}. Disponible en: (http://www.webopedia.com/TERM/F/firewall.html).

BURGUAN VALVERDE, Iliana Maritza. Recursos universitarios de Iliana Burguan. {En línea}. {24 de Febrero de 2015}. Disponible en: (https://ilianaburguan.wordpress.com/2010/01/08/hardening-de-windows/).

CASTILLA, José. Comprueba qué puertos tiene abiertos {En línea}. {5 de Abril de 2015}. Disponible en: (http://www.softzone.es).

CASTRO, Paul. Blog.smartekh. {En línea}. {8 de Febrero de 2015}. Disponible en: (http://blog.smartekh.com/%C2%BFque-es-hardening/).

CEQUEDA, Jean Pole. Robo de información mediante la interceptación de mensajes. {En línea}. {12 de Marzo de 2015}. Disponible en: (https://seguridadinformaticaufps.wikispaces.com/ROBO+DE+INFORMACI%C3%93N+MEDIANTE+).

COLASOFT. What is a Sniffer? {En línea}. {12 de Mayo de 2015}. Disponible en: (http://www.colasoft.com/resources/sniffer.php).

CRISTIAN, Borghello. Detección de Intrusos en Tiempo Real. {En línea}. {3 de Mayo de 2015}. Disponible en: (http://www.segu-info.com.ar/proteccion/deteccion.htm).

CYRILLE, Larrieu. Sistema de Detección de Intrusiones. {En línea}. {3 de Agosto de 2015}. Disponible en: (http://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids).

DCSSI. La defensa en profundidad aplicada a los sistemas de información. {En línea}. {19 de Mayo de 2015}. Maubourg: s.n.2004.

DEL RIO, Mariano M. La importancia de conocer el entorno a proteger {En línea}. {4 de Abril de 2015}. Disponible en: (https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/la_importancia_de_conocer_el_entorno_a_proteger?realLang=fr).

FEBLES RODRÍGUEZ, Juan Pedro. Criptografía y Redes. {En línea}. {1 de Agosto de 2015}. Disponible en: (http://maestriainformaticamg.blogspot.com.co/2012/07/presentacion-tema-5.html).

FERRAN, Pelechano. Bloqueo De Puertos En Comtrend HG536+. {En línea}. {26 de Abril de 2015}. Disponible en: (http://www.pelechano.com/wp-content/uploads/2011/08/puertos.png).

FORMACIÓN, Líderes Nacionales de Cadena La Investigación en la Escuela de Ciencias Básicas, Tecnología e Ingeniería {Informe}. Bogotá D.C.: Universidad Nacional Abierta y a Distancia –UNAD, 2011.

FUNDACIONCTIC. Medidas de seguridad básica: Los puertos de tu router. {En línea}. {15 de Mayo de 2015}. Disponible en:

(http://www.fundacionctic.org/sat/articulo-medidas-de-seguridad-basicas-los-puertos-de-tu-router).

G_SMARTEKH. Qué_es_hardening. {En línea}. {12 de Enero de 2015}. Disponible en: (http://blog.smartekh.com).

GCFAPRENDELIBRE. ¿Qué son los antivirus? {En línea}. {19 de Febrero de 2015}. Disponible en: (http://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_antivirus/1.do).

HUMISTON, Michael. Zenmap Scan. {En línea}. {6 de Julio de 2015}. Disponible en: (http://michaelhumiston.com/wp-content/uploads/2011/03/zenmap2.png).

INFOSEGUR. Criptografía. {En línea}. {9 de Mayo de 2015}. Disponible en: (https://infosegur.wordpress.com/category/4-criptografia/).

IP, Soluciones. Firewall Cortafuegos. {En línea}. {8 de Febrero de 2015}. Disponible en: (http://soluciones-ip.pe/firewall-cortafuegos).

IP Soluciones, Img_Firewall-Cortafuegos. {En línea}. {15 de Febrero de 2015}. Disponible en: (http://soluciones-ip.pe/ip/wo-content/uploads/2014/07/f1.jpg).

IRE. Qué componentes Hardware tiene tu PC. {En línea}. {16 de Mayo de 2015}. Disponible en: (http://adnfriki.com/saber-que-componentes-hardware-tiene-tu-pc/).

JIMENEZ SOTO, León Manuel. Redes de Área Local: Sniffers o Analizadores de Paquetes. {En línea}. {27 de Agosto de 2015}. Disponible en: (https://infosegur.wordpress.com/category/4-criptografia/).

KIOSKEA, Ids. {En línea}. {22 de Abril de 2015}. Disponible en: (http://es.kioskea.net).

LYON, Gordon. Obtaining, Compiling, Installing, and Removing Nmap. {En línea}. {12 de Mayo de 2015}. Disponible en: (https://nmap.org).

MARTINEZ RODRÍGUEZ, Lorenzo. La importancia del bastionado de sistemas. {En línea}. {25 de Junio de 2015}. Disponible en: (https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/importancia_bastionado_sistemas?realLang=fr).

MICROSOFT. Amenazas y Contramedidas. {En línea}. {3 de Abril de 2015}. Disponible en: (https://technet.microsoft.com).

MICROSOFT. Descripción de la configuración de Firewall de Windows. {En línea}. {23 de Enero de 2015}. Disponible en: (http://windows.microsoft.com).

MIRA ALFARO, Emilio José. Implantación de un sistema de detección de intrusos en la Universidad de Valencia. {En línea}. {24 de Marzo de 2015}. Disponible en: (http://rediris.es/cert/doc/pdf/ids-uv.pdf).

MONTANAN, Rogelio. Redes, trabajos IDS. {En línea}. {18 de Junio de 2015}. Disponible en: (www.uv.es/~montanan/redes/trabajos/IDSs.doc).

PARSON, Lexers. Modelo de seguridad en Profundidad. {En línea}. {21 de Junio de 2015}. Disponible en: (http://www.guatewares.com/2014/04/modelo-de-seguridad-en-profundidad.html).

RHO5223. Mejorar la seguridad de Windows mediante el cierre de puertos abiertos {En línea}. {10 de Julio de 2015}. Disponible en: (http://geexone.blogspot.com.co/2010/04/mejorar-la-seguridad-de-windows.html).

RIOS, Julio. Restricciones en el Firewall. {En línea}. {27 de Febrero de 2015}. Disponible en: (http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml).

ROBAYO L, Javier Humberto. Políticas de Seguridad. {En línea}. {12 de Junio de 2015}. Disponible en: (http://jhrlsegredes.blogspot.com/).

ROBBINS STEPHEN & COULTER Mary Administración {Sección de libro}. México: Pearson-Prentice Hall}.8VA.:1., 2005.

S. NORTHCUTT D. McLachlan y J. Novak Network Intrusion Detection: An Analyst's handbook {En línea}. {28 de Abril de 2015}. Disponible en: (www.uv.es/~montanan/redes/trabajos/IDSs.doc).

SÁNCHEZ, Eduardo. Patricio Hardening. {En línea}. {14 de Enero de 2015}. Disponible en: (http://www.magazcitum.com.mx/?p=2109).

SEGURA, Benjamín. Simple Port Tester. {En línea}. {19 de Marzo de 2015}. Disponible en: (http://cdn6.portalprogramasnet.com/imagenes/programas/es/757/9757_1.jpg).

SITIOSARGENTINA. Qué es un Antivirus. {En línea}. {6 de Abril de 2015}. Disponible en: (http://www.sitiosargentina.com.ar).

TARLOGIC. Bastionado de sistemas (hardening). {En línea}. {4 de Julio de 2015}. Disponible en: (https://www.tarlogic.com/servicios/bastionado-de-sistemas-hardening/).

THOMSON, Ivan. Definición de Administración. {En línea}. {9 de Mayo de 2015}. Disponible en: (http://www.promonegocios.net/administracion/definicion-administracion.html).

TIPOSDE.ORG. Tipos de Virus Informáticos. {En línea}. {15 de Abril de 2015}. Disponible en: (http://www.tiposde.org).

TRENDCORP. Preventor de Intrusos. {En línea}. {4 de Junio de 2015}. Disponible en: (http://www.trendcorp.com.pe/img/dummies/intruso.jpg).

TRIPOD. Seguridad Y Protección En Sistemas Operativos De Propósito General. {En línea}. {14 de Julio de 2015}. Disponible en: (http://profinal0.tripod.com/seguridad.htm).

UNTIVEROS, Sergio. Sniffing. {En línea}. {27 de Junio de 2015}. Disponible en: (http://www.aprendaredes.com).

UPTODOWN. Conoce qué puertos TCP y UDP utiliza tu equipo. {En línea}. {3 de Julio de 2015}. Disponible en: (http://currports.uptodown.com).

VITRIAGO, Michael. Virus y antivirus de computadora. {En línea}. {14 de Marzo de 2015}. Disponible en: (http://www.monografias.com/trabajos94/virus-y-antivirus-pc/virus-y-antivirus-pc.shtml).

ANEXO A
EJEMPLO DE AUDITORÍA TÉCNICA

AUDITORÍA TÉCNICA

INTRODUCCIÓN

El procedimiento de auditoría técnica hace referencia a evaluar el estado de sistema operativo y sus configuraciones de seguridad, a diferencia de una auditoria de seguridad de la información esta logra determinar técnicamente dificultades y limitaciones frente a la protección en profundidad de ataques informáticos. Para este proceso es importante tener claro que debemos partir del concepto de defensa en profundidad ya que un test de pruebas de seguridad o ética hacking solo determina las vulnerabilidades a nivel de RED por lo cual pueden ser muchas las variables que no se puedan tener en cuenta a la hora de hacer un aseguramiento un profundidad. Cabe recordar que este proyecto enfatiza el concepto de “DEFENSA EN PROFUNDIDAD”, por lo cual el aseguramiento debe ser desde el corazón del sistema operativo y no desde el exterior para poder enfrentar al sistema operativo y al atacante en determinado momento y este logre minimizar proactivamente el ataque.

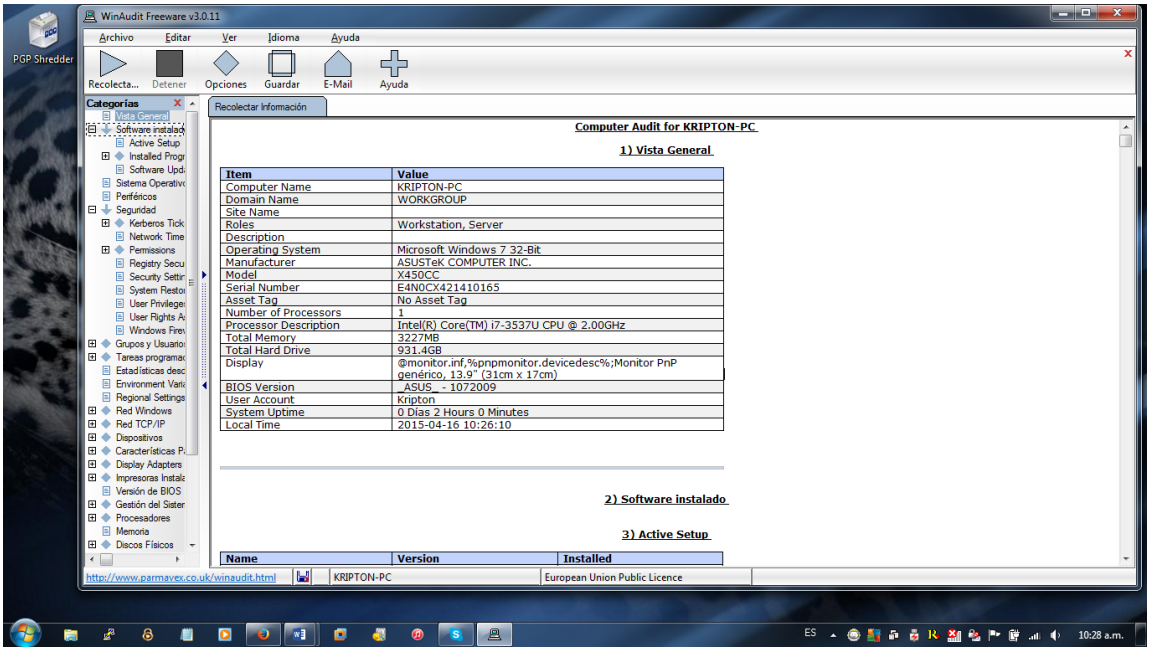
A continuación vemos un ejemplo de registro de Auditoría Técnica:

Herramienta de auditoria: WINAUDIT

Equipo Administrador: KRIPTON-PC

Descripción: Equipo administrador de servidor WEBHOSTING, el cual se encuentra en un datacenter en Estados Unidos, este servidor tiene carácter de arrendamiento y solo se tiene acceso por medio de conexiones SSH.

Registro de información básica del sistema:



Objeto 01. *Descripción:* En este objeto se describe detalladamente la configuración del sistema operativo, relacionando la información básica del sistema, números de seriales e ID del sistema.

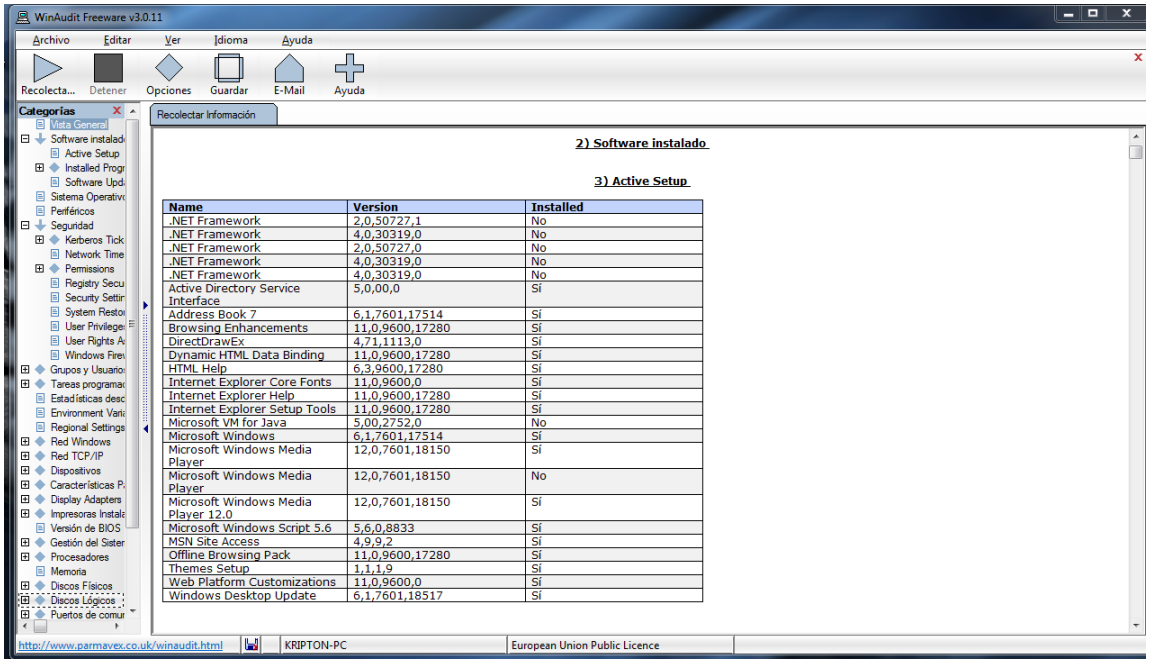
Software instalado

En esta verificación lo que se debe determinar es el software que posiblemente sea malicioso, por lo cual se debe tener una bitácora de instalación y de administración

de este para poder comparar y verificar cambios malignos que puedan estar en el sistema operativo.

Cabe resaltar que esta actividad NO verifica si realmente está infectado el sistema ya que el sistema antes de hacer esta verificación puede tener un troyano o rootkit instalado el cual pueda camuflarse en los ejecutables ya activos, esta verificación evalúa si se instaló algún software adicional a los permitidos según se defina una política de seguridad de instalación de software en los sistemas operativos.

Adicional a esto se puede identificar que software se debería actualizar para tener un marco claro de actualizaciones a nivel estadístico.

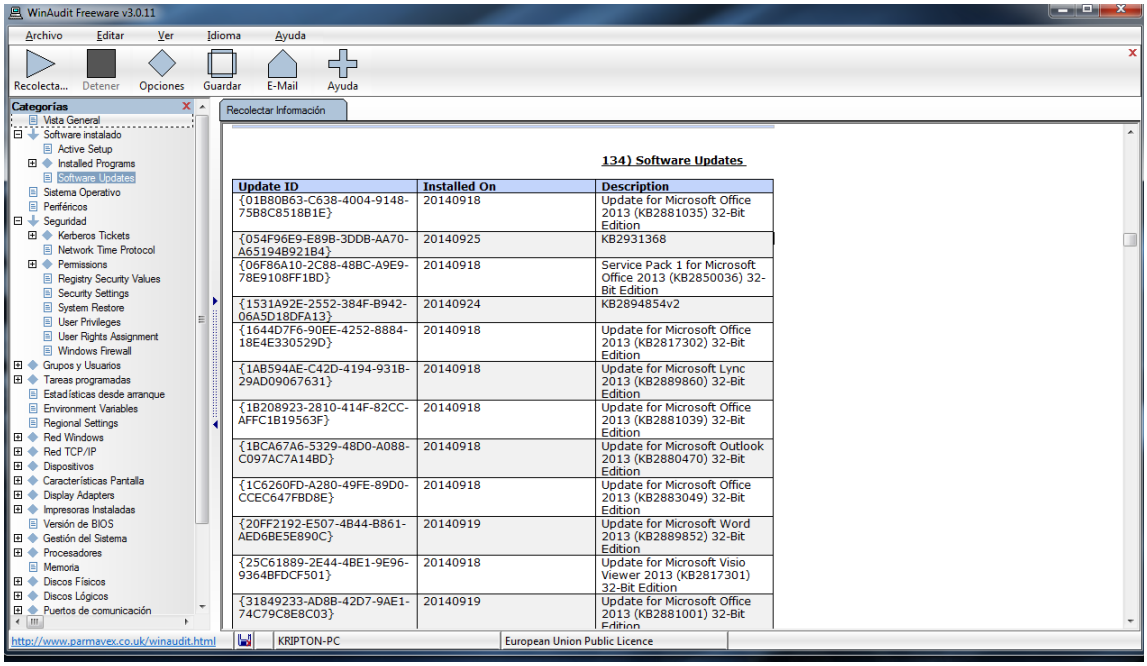


Objeto 02. *Descripción:* El objeto 02 nos ilustra los diferentes programas que están instalados en el sistema operativo mostrando su nombre y versión de instalación.

Updates de sistema operativo

Las actualizaciones hacen parte esencial y determinante a la hora de hacer un aseguramiento tecnológico o Hardening, por ello esta actividad nos apoya brindando información importante para tener actualizado el sistema operativo, este

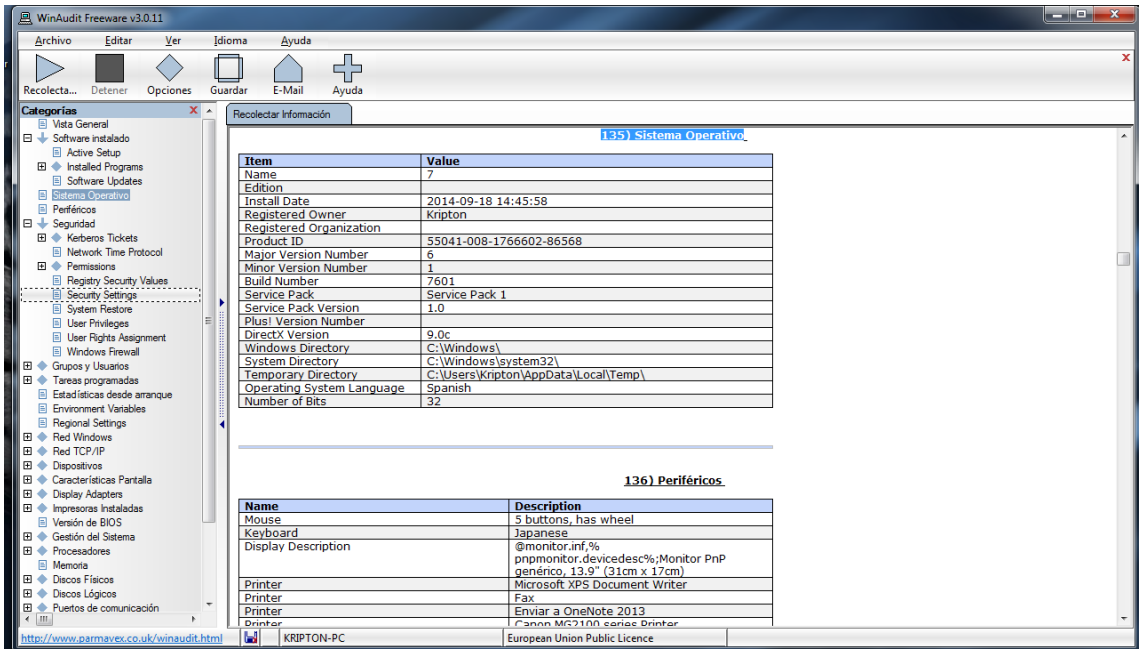
registro permite tener un ambiente claro de lo que se debe fortalecer con estas actualizaciones.



Objeto 03. *Descripción:* Aquí se representa las diferentes actualizaciones del sistema operativo, con esta información es posible comparar las últimas versiones para poder determinar actualizaciones significativas de seguridad.

Información de sistema operativo

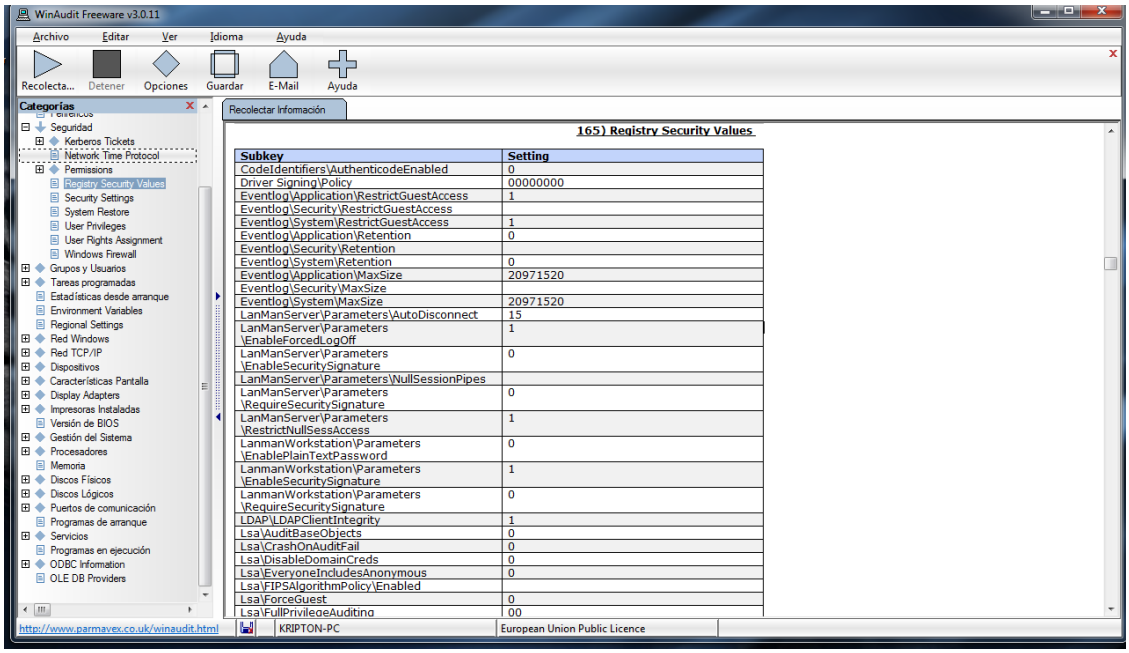
La información que se visualiza en este paso nos indica que sistema operativo y el service pack el cual nos indica en que versión del sistema podemos aplicar actualizaciones.



Objeto 04. *Descripción*: La información contenida en este ítem nos aporta datos de carpetas y rutas por defecto del sistema operativo, bajo que bit corre el sistema operativo versiones de servicie pack y el lenguaje de sistemas.

Verificación del registro de Windows

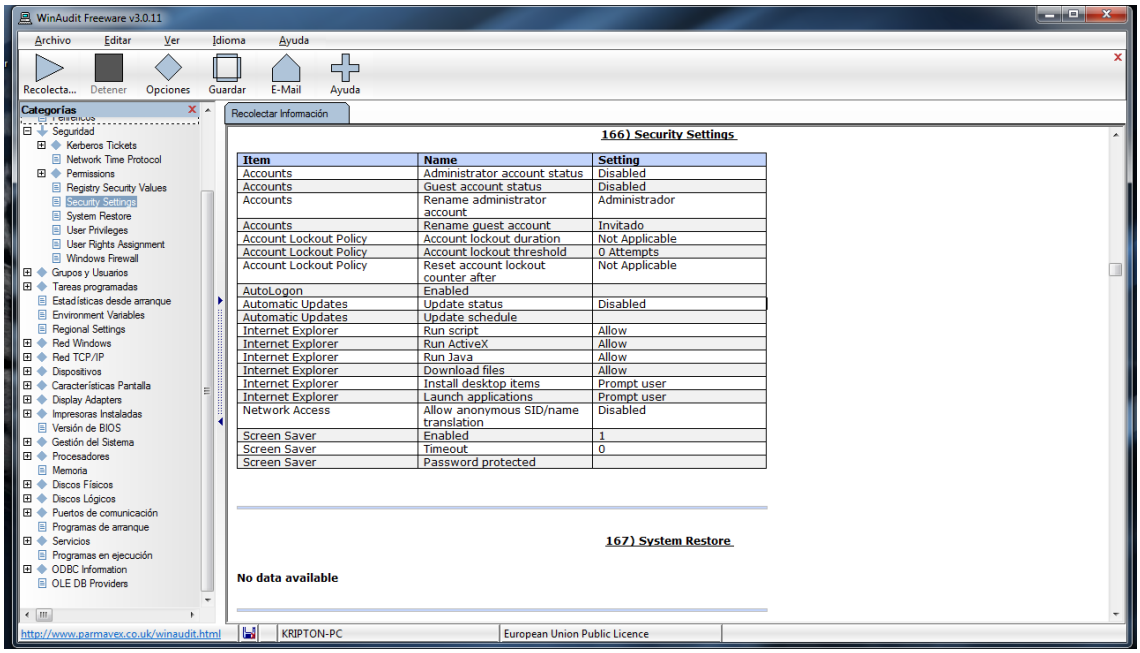
Este es un elemento muy importante a la hora de verificar si existen posibles alteraciones en el sistema operativo y posibles intrusiones ya que aquí se determinan los procesos y funciones que interactúan con el sistema operativo.



Objeto 05. *Descripción*: La importancia de conocer los parámetros del registro de Windows es de vital importancia en la seguridad ya que los virus para ser persistentes lo deben utilizar alterándolo, por lo cual este objeto nos indica modificaciones de registro en caso de que este alterado, esto se debe analizar con un backup del registro para poder comprar cambios de los parámetros.

Configuración de Seguridad del sistema

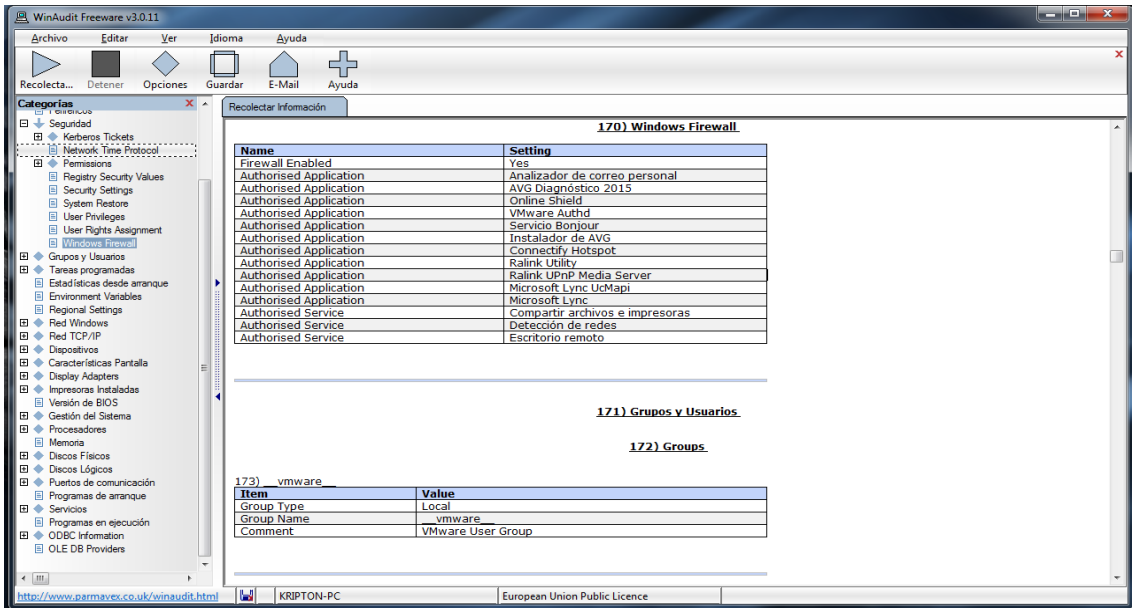
Este ítem es importante para saber que usuarios con permisos administrativos están activos y pueden llegar a ser puerta de entrada de los atacantes.



Objeto 06. *Descripción*: El objeto 06 nos da información relacionada con la seguridad del sistema donde nos da información cuantas de usuarios creadas, grupos y permisos al sistema.

Firewall de Windows

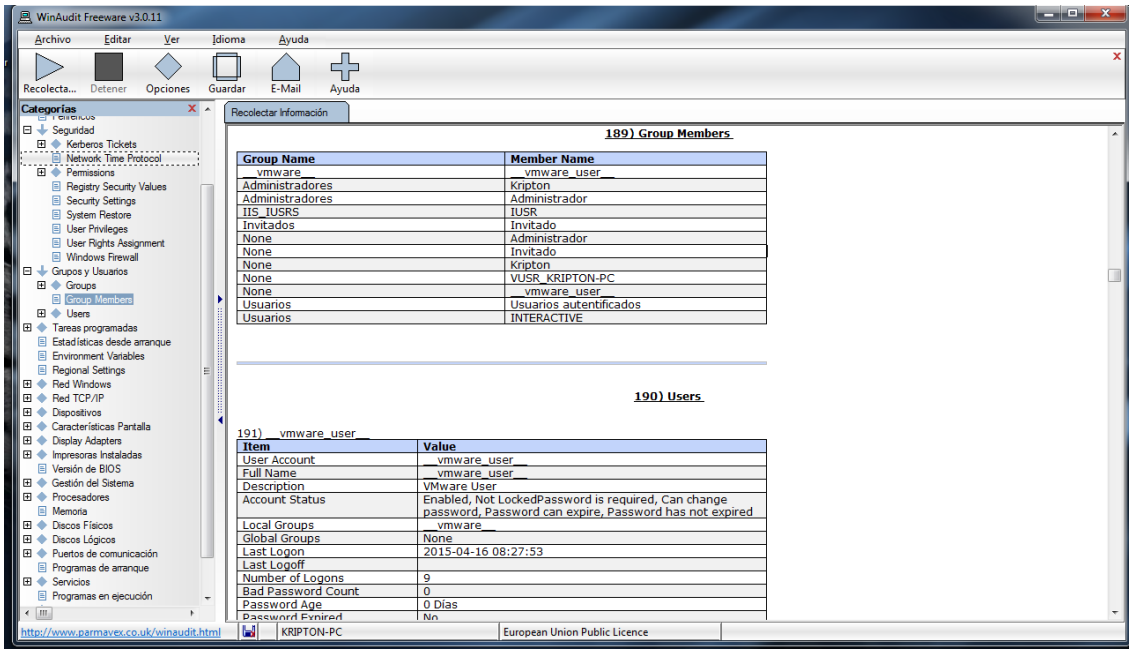
El firewall es un elemento importante a la hora de contrarrestar ataques informáticos ayudando a bloquear entradas remotas hacia el sistema operativo, aquí podemos verificar si se encuentra activo e igualmente sus módulos que apoyan su verificación.



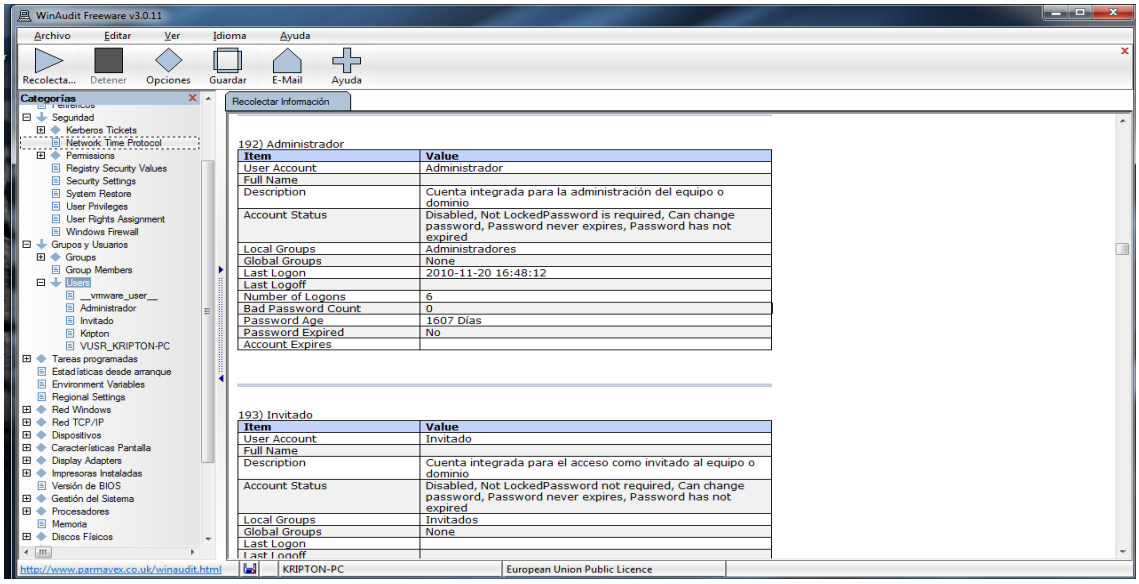
Objeto 07. *Descripción*: Los parámetros de seguridad de firewall de host nos informa de accesos que se deben boquear y los que están bloqueados, este objeto nos da información de las aplicaciones autorizadas como servicios o procesos del sistema.

Grupos de sistema

Los grupos del sistema permiten igualmente identificar que usuarios tienen permisos de administrador, los permisos de este tipo regularmente son los más vulnerables ya que cuentan con la posibilidad de modificar argumentos de las aplicaciones del sistema o dar paso a cambios del sistema operativo.



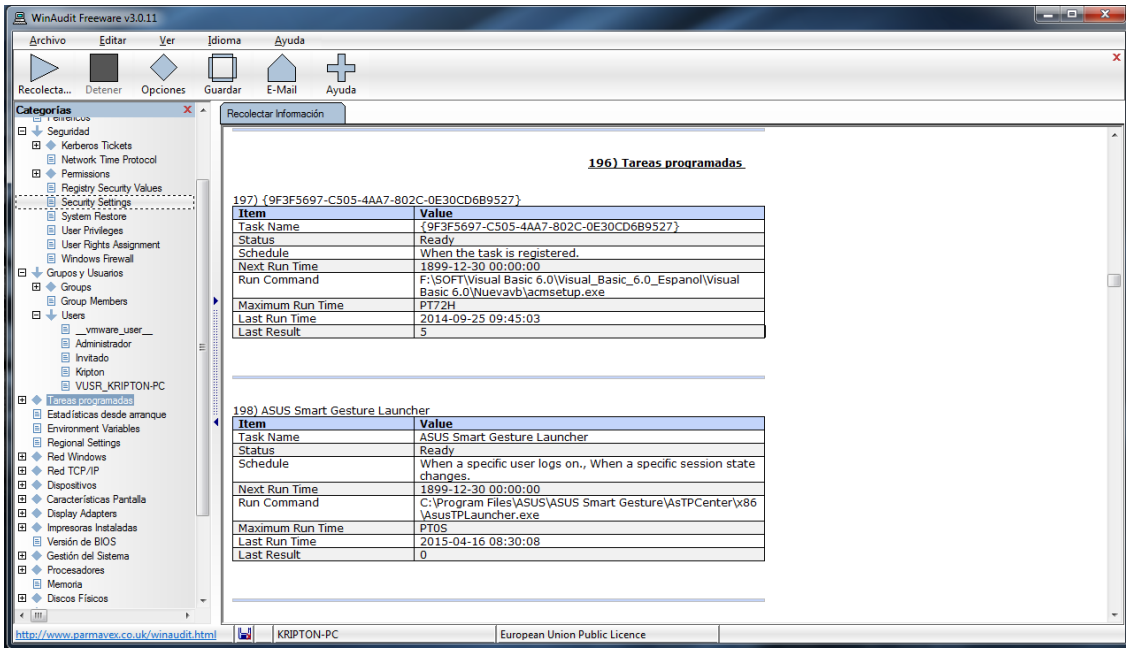
Objeto 08. *Descripción*: Los permisos de los grupos del sistema deben estar perfectamente configurados para evitar asignar roles que puedan realizar cambios al sistema operativo, por ello este objeto nos da información de que usuarios y que permisos están agregados al sistema operativo.



Objeto 09. *Descripción*: Aquí nos da información de los usuarios administradores, se debe tener cuidado y definir bien las políticas de seguridad para agregar estos usuarios al sistema.

Tareas programadas

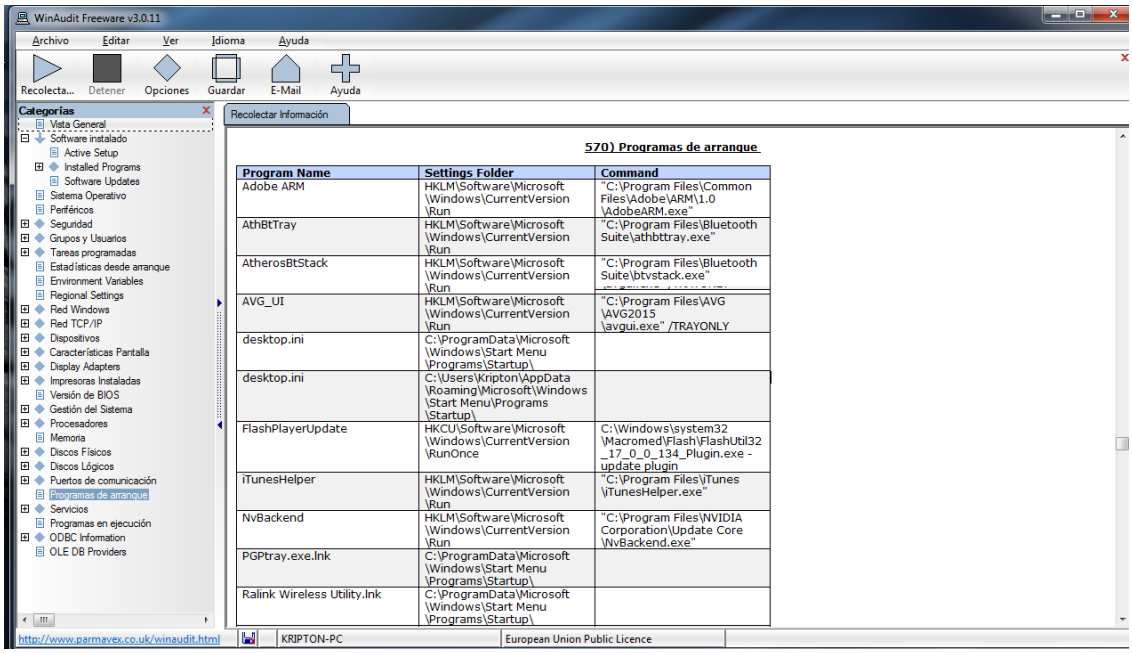
Las tareas programadas definen los procesos que se ejecutaran en algún determinado momento, con esto el atacante puede practicar un paso que se denomina mantener el objetivo, ya que puede programar determinados procesos para mantener el virus activo o inclusive actualizarlo, por lo cual la verificación de este ítem es importante para evitar sostenibilidad de virus o rootkits.



Objeto 10. *Descripción*: Este objeto nos da información de las tareas programadas del sistema operativo, estas tareas son importante a medida de que sean taras de administración del sistema pero pueden alterarse por un virus para lograr mantenerse o propagarse en el sistema operativo.

Programas de arranque

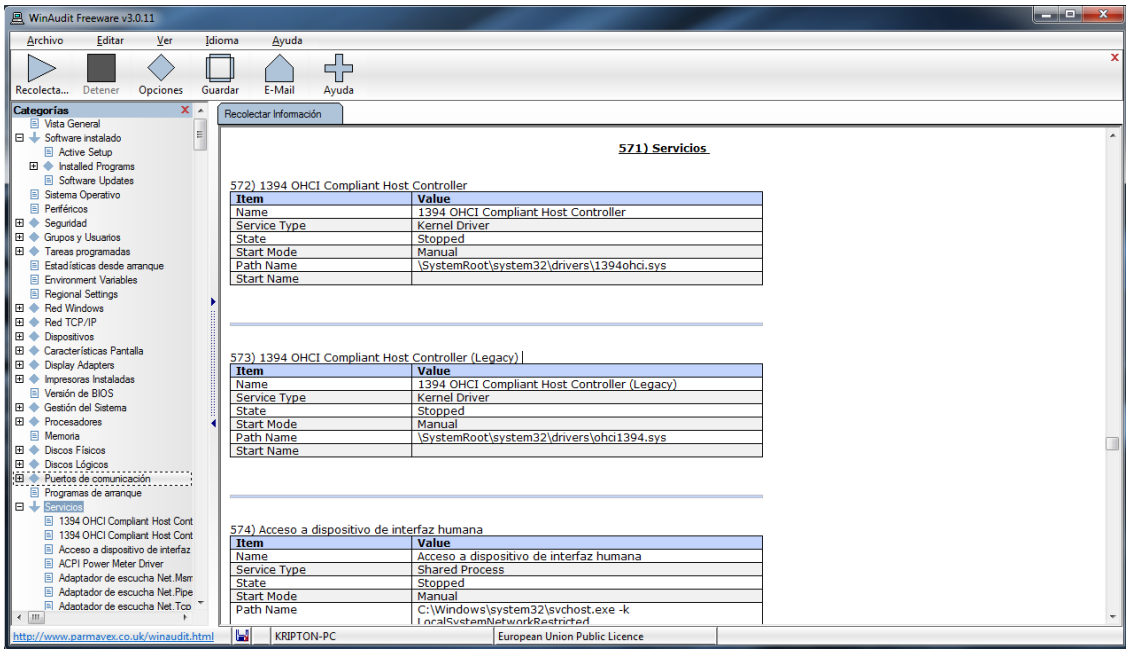
Los ataques informáticos deben tener como objetivo el mantener el acceso para poder tener control del sistema operativo para ellos utilizan diferentes técnicas que permiten controlar el sistema en el tiempo. Las claves de arranque de registro de Windows permite practicar uno de esos objetivos ya que por medio de este el virus o troyano iniciar al arrancar el sistema operativo o que hace que se active si necesidad de volver a instalarlo.



Objeto 11: *Descripción*: El sistema de arranque ilustrado en el objeto 11, da información de los programas que se inician en el arranque del sistema operativo, esto debe ser cuidadosamente analizado ya que la gran mayoría de virus se copia a este proceso donde los hace persistentes en el sistema operativo.

Servicios de sistema

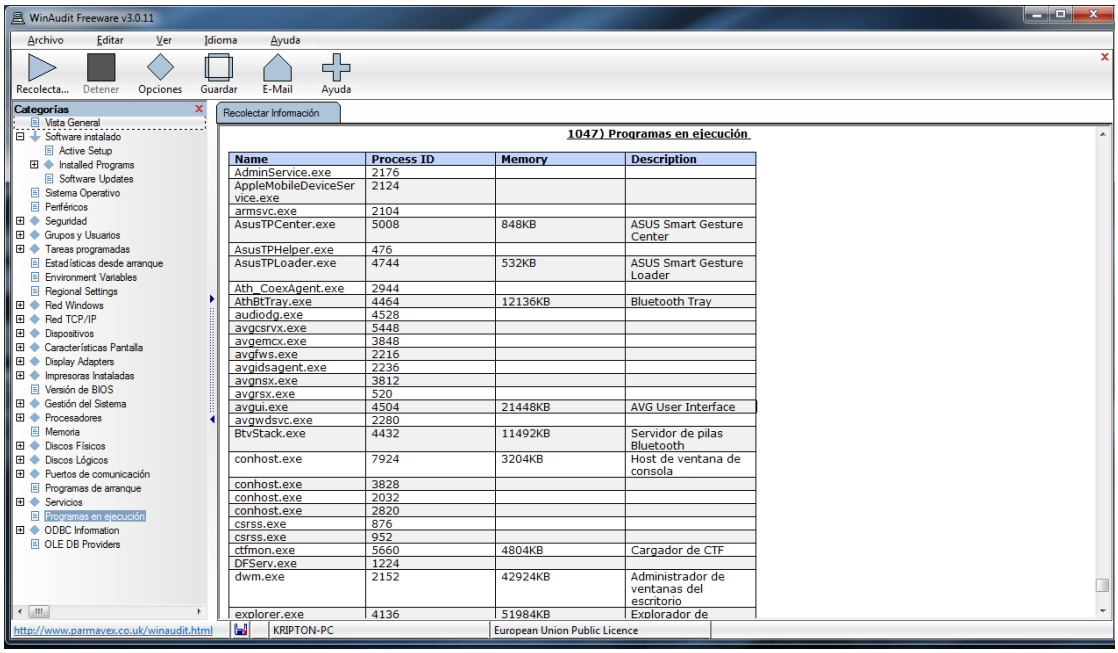
Para el sistema los servicios son los que gestionan los procesos del sistema operativo, por ellos es importante evaluar cuáles son los servicios por defecto del sistema y los que genera cada aplicación al ser activa, esto con el fin de identificar instalación de malware.



Objeto 12. *Descripción*: Los procesos del sistema son parte de información de los programas que están activos en el sistema operativo, por ello este objeto nos da información de los procesos activos en el momento, aquí es posible determinar qué proceso no es del sistema para determinar si el sistema operativo fue vulnerado.

Programas en ejecución

Con esto se verifica los programas que están activos actualmente en el sistema, aquí se puede identificar software que este corriendo con intenciones de daño al sistema operativo o la información.



Objeto 13. *Descripción*: Aquí el objeto nos informa que programas se encuentran activos en el sistema, existen métodos de vulneración basados en caballos de Troya donde los virus se mezclan con programas originales del sistema aquí podemos observar el comportamiento de estos programas y ver si se encuentran troyanizados, esto se identifica porque se puede ver corriendo el programa en modo oculto.

CONCLUSION

La verificación de los diferentes elementos de seguridad y configuraciones en los sistemas operativos hacen parte del procedimiento de aseguramiento, tener en cuenta la aplicación de políticas de seguridad y la buena configuración del sistemas permite tener un grado de confianza para poder generar un buen funcionamiento en el sistema.

Los ataques en profundidad regularmente son ataques agresivos y que hacen parte de una estrategia planeada y desarrolla muy técnicamente, con el fin de lograr el objetivo final que es explotar vulnerabilidades y mantener el sistema controlado, por ello se debe implementar un proceso técnico de aseguramiento que combinado con políticas de seguridad permita estabilidad y armonía entre el usuario y el sistema operativo.

REFERENCIAS

WINAUDIT. {En línea}. {3 de Febrero de 2015}. Disponible en: (https://winaudit.codeplex.com/). Tipo de licencia: Gratuita (FREEWARE). Versiones: 3.0.11, 3.0.10, 3.0.9, 3.0.8, 3.0

ADMIN. Análisis completo de tu equipo con Winaudit. {En línea}. {9 de Febrero de 2015}. Disponible en: *(*https://cajondesastres.wordpress.com/2010/01/05/analisis-completo-de-tu-equipo-con-winaudit/).

GURU63. WinAudit: Cómo hacer un inventario de las características de hardware y software de la computadora. {En línea}. {27 de Febrero de 2015}. Disponible en: (http://www.guru63.com/winaudit-come-fare-un-inventario-delle-caratteristiche-hardware-e-software-del-computer/).

HAMT. Auditoria de sistemas (WINAUDIT). {En línea}. {14 de Febrero de 2015}. Disponible en: (https://www.powtoon.com/show/di3J2IihNYy/auditoria-de-sistemas-winaudit/).