ESTUDIO SOBRE LA APLICACIÓN DE HARDENING PARA MEJORAR LA SEGURIDAD INFORMÁTICA EN EL CENTRO TECNICO LABORAL DE TUNJA – COTEL

JAISON DUVANY FACHE MONTAÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACION EN SEGURIDAD INFORMATICA
TUNJA, COLOMBIA
2016

ESTUDIO SOBRE LA APLICACIÓN DE HARDENING PARA MEJORAR LA SEGURIDAD INFORMÁTICA EN EL CENTRO TECNICO LABORAL DE TUNJA – COTEL

JAISON DUVANY FACHE MONTAÑA

Trabajo de grado como requisito para optar el título de Especialista En Seguridad informática

Director
HERNANDO JOSE PEÑA HIDALGO
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACION EN SEGURIDAD INFORMATICA
TUNJA, COLOMBIA
2016

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Tunja 22 de abril de 2017

DEDICATORIA

El presente trabajo es dedicado a mis padres por su apoyo y amor incondicional, y a mis hermanos por ser los maestros de mi vida.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

TITULO

ESTUDIO SOBRE LA APLICACIÓN DE HARDENING PARA MEJORAR LA SEGURIDAD INFORMÁTICA EN EL CENTRO TECNICO LABORAL DE TUNJA – COTEL

INTRODUCCION

Desde el comienzo de la computación una de las razones fundamentales de la informática ha sido la seguridad de la información; el surgimiento de ataques virales, robo de información, o daño a equipos computacionales afectan hoy día a las empresas en torno a sus activos informáticos y de paso limitan las operaciones administrativas de las mismas.

Así pues, el hardening se presenta como una de las medidas más importantes de seguridad a implementar en toda organización, ya que permite establecer distintas barreras de protección frente a los posibles atacantes, ya sean tanto a nivel externo (amenazas desde las redes e internet), así como atacantes internos, (personas que hacen uso del sistema internamente), señalando que algunos de ellos pueden ser simplemente personas que ocasionan daños sin intención o por indebida manipulación de los equipos informáticos.

El hardening o bastionamiento, entendido como un proceso que implica la implementación de medidas de seguridad tanto en hardware como en software requiere por tanto de la generación de barreras preventivas para evitar daños a un sistema informático y teniendo como referencia el instituto Cotel de Tunja, se brinda un espacio para proponer aplicaciones y métodos que ayuden a robustecer la seguridad informática a partir de la aplicación de un análisis preliminar de vulnerabilidades y deficiencias; igualmente es importante mencionar que los resultados surgidos de este estudio pueden ser implementados en toda organización que tenga un sistema informático a proteger.

1. DEFINICIÓN DEL PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA

El Centro De Formación Técnico Laboral De Tunja – COTEL, es una institución de educación para el trabajo y el desarrollo humano, debido a esto se ha implementado una serie de ayudas tecnológicas para hacer más eficiente la labor administrativa y el desarrollo educacional, es así que se emplean tanto equipos informáticos (computadores, impresoras, redes, switches, etc.) como también aplicaciones para el desarrollo de las labores académicas y laborales (sistemas operativos, paquetes ofimáticos, hojas de caculo, bases de datos entre otros); de lo anterior, dependen 600 estudiantes semestralmente (en promedio) y 65 empleados anualmente, no obstante, muchas de las labores realizadas alrededor de estas ayudas tecnológicas no son realizadas de forma idónea ya que no garantizan el funcionamiento correcto de los dispositivos informáticos ni aseguran las máximas de la seguridad informática frente a protección de datos como son la disponibilidad, integridad de los datos y confidencialidad de los mismos.

Lo anteriormente mencionado ha llevado al instituto a poner en riesgo sus procesos tanto a nivel laboral como académico al no poder brindar un desarrollo eficiente de los procesos tecnológicos y es razón por la cual se hace necesario el realizar un estudio con el fin de proponer medidas de seguridad a partir del análisis y entendimiento del proceso de hardening para encontrar opciones de seguridad informática que coadyuven al aseguramiento de su sistema informático.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo la aplicación de un proceso de hardening permitirá mejorar la seguridad informática en el Centro Técnico Laboral de Tunja - COTEL?

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Realizar un estudio del nivel de seguridad en la red informática, para la implementación de medidas basadas en hardening, que permitan mejorar la seguridad informática en el Centro Técnico Laboral de Tunja – COTEL

2.2. OBJETIVOS ESPECÍFICOS

- Indagar en diferentes fuentes de información acerca del proceso de hardening señalando la aplicabilidad, ventajas, estrategias y técnicas del mismo, a la vez que se reconocerá la importancia del concepto de defensa en profundidad respecto del modelo promovido por Microsoft, las capas que lo componen y su modo de aplicabilidad.

- Estudiar herramientas y medidas de hardening en estaciones de trabajo tipo Windows describiendo características y usos de las mismas.

- Identificar herramientas y medidas de hardening para estaciones de trabajo basadas en ambientes Linux reconociendo la aplicabilidad de estas.

- Presentar a través de un informe, las respectivas recomendaciones para mejorar la seguridad informática del instituto COTEL-TUNJA de acuerdo al modelo de defensa en profundidad promovido por Microsoft.

3. JUSTIFICACIÓN

La aplicación de las tecnologías de la información y la comunicación (TIC) en la actualidad es una necesidad de toda empresa ya que implica directamente la sistematización de la información con el fin de reducir costes y agilizar procesos administrativos. No obstante, con el desarrollo y aplicación de estas tecnológicas, es de esperar que se presenten falencias en las mismas no solo por el mal uso, sino también por la falta de medidas preventivas frente a los posibles ataques informáticos; este motivo obliga a realizar un aseguramiento de la información que garantice la disponibilidad, confidencialidad e integralidad de la misma.

En el caso de instituciones educativas, las TIC se presentan como una de las estructuras fundamentales sobre todo por el desarrollo tecnológico del país en la última década, lo cual ha sido impulsado en buena parte por los últimos gobiernos; esto implica que en una institución como COTEL, los equipos informáticos y sus respectivos aplicativos deben ser brindados a su comunidad estudiantil de la forma más óptima y segura posible.

El hardening entonces se expone como una excelente respuesta para el aseguramiento del sistema informático de una organización, toda vez que robustece un sistema informático haciendo uso de barreras o bastiones, sean en hardware o en software, que garantizan medidas efectivas frente a ataques o daños.

Teniendo en cuenta que los problemas informáticos de una organización no son exclusivos de esta sino que pueden ser problemas que cualquier entidad puede llegar a afrontar, se hace necesario el realizar un estudio sobre la aplicación de hardening para mejorar la seguridad informática donde los resultados obtenidos del mismo puedan beneficiar a otras organizaciones o usuarios de sistemas informáticos, así como a expertos en sistemas e informática que busquen opciones en la protección de sus sistemas, lo cual igualmente conllevará a que este estudio se convierta en fuente de consulta.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Reconociendo la importancia del hardening y su aplicación en sistemas informáticos para hacer frente a amenazas o daños, y teniendo en cuenta la necesidad de realizar un estudio sobre las opciones que se pueden implementar alrededor de ello, se plantea que este proyecto abarque toda la planta informática del instituto COTEL de la ciudad de Tunja, con el fin de mejorar el nivel de seguridad informática de la misma y aumentar con ello la satisfacción de los usuarios tanto internos como externos de la institución frente al servicios educativos, así como garantizar la seguridad de la información en el ámbito administrativo de esta organización.

Es por ello que dichas acciones se realizarán en las instalaciones del instituto COTEL de la ciudad de Tunja, municipio del departamento de Boyacá y la población beneficiada serán los estudiantes y trabajadores administrativos del mismo señalando como tiempo de desarrollo de este proyecto periodo de 4 meses durante el año 2016.

Es de mencionar que a lo largo del proyecto se hablará de COTEL-TUNJA ubicado en la ciudad de Tunja (Boyacá) y en la cual se centra el proyecto, esto debido a que existe otra sede del instituto en la ciudad Duitama (Boyacá), razón por la cual se hace necesario su diferenciación y delimitación.

5. MARCO REFERENCIAL

5.1. ANTECEDENTES

Centrados en el tema investigación respecto de hardening, se encontraron distintos documentos e investigaciones implementados en diferentes lugares y países los cuales han tratado referencias y discusiones frente a este estudio en lo que tiene que ver con las diferentes opciones de aseguramiento de sistemas.

El trabajo “Desarrollo de una guía para selección y endurecimiento (hardening) de sistemas operativos para un centro de datos”[1], publicado por Omar Sánchez, habla de la normatividad que se puede implementar alrededor del aseguramiento de sistemas teniendo en cuenta NIST e ISO 15408, así como el estándar FSI. De igual forma menciona el desarrollo preliminar de una guía de hardening a partir del estándar FSI integrando ISO 27002 y COBIT 4.1 a la vez que genera una serie de procedimientos operativos estandarizados (POE). Igualmente reseña el cumplimiento del software utilizado en una organización de acuerdo al common criteria de ISO 15408.

El trabajo “Aseguramiento de los sistemas computacionales de la empresa sitiosdima.net” publicado por Javier Robayo y Richar Rodríguez”[2]. Hace referencia a la implementación de un proceso de hardening a través del aseguramiento del sistema computacional de una empresa que brinda servicios web; en este se estudian conceptos básicos sobre sistemas operativos Windows, modo de funcionamiento y parcheos de seguridad. Por otro lado, trata el tema de defensa en profundidad y su modo de aplicación teniendo presente temas como virus informáticos, métodos de infección, principales medios antivirales y la clasificación de éstos. Este trabajo se centra específicamente en medidas de seguridad alrededor de Windows toda vez que trata acerca del manejo del firewall de este sistema y se plantea un cerramiento de puertos en a través del mismo habiéndose ejecutado un escaneo de puertos anteriormente. De igual manera, trata el hardening por fuera de Windows como la implementación de IDS, sistemas de contraseñas seguras, criptografía, sniffers, así como políticas y buenas prácticas de seguridad informática.

[1] SANCHEZ, O. (2011). Desarrollo de una guía para selección y endurecimiento (hardening) de sistemas operativos para un centro de datos. 2016, de IPN –México. Disponible en: http://tesis.ipn.mx/jspui/handle/123456789/8466

[2] ROBAYO, J. (2015-01-04). Aseguramiento de los sistemas computacionales de la empresa Sitiosdima.net. Disponible en: http://hdl.handle.net/10596/3818

La tesis “Diseño e implementación de un esquema de seguridad perimetral. Para redes de datos caso práctico: dirección general del colegio ciencias y humanidades”[3] presentado por José Baltazar y Juan Campuzano. Este trabajo en su “capítulo 4. Buenas prácticas de seguridad”, menciona el por qué invertir en la seguridad de un sistema informático, señalando la importancia de hacer uso correcto de los medios informáticos así como de las redes que los interconectan, de igual manera señala una serie de medidas en cuanto a políticas de seguridad para robustecer un sistema informático, indicando buenas prácticas de administración de seguridad con base en estándares, seguridad en redes, backups, y protección frente a dispositivos removibles y pentesting. Igualmente es de resaltar el aparte respecto de hardening en sistemas operativos Microsoft y Unix-Linux en el que hace profundidad acerca de la disponibilidad de herramientas y técnicas para robustecer la seguridad informática resaltando el factor de la concientización de los usuarios finales para que hagan parte del esquema de seguridad.

5.2. MARCO TEÓRICO

5.2.1. Educación para el trabajo y el desarrollo humano. La Educación para el Trabajo y el Desarrollo Humano es un servicio público educativo enmarcado dentro de la Ley 115 de 1994, el cual busca complementar y suplir conocimientos con el fin de permitir la obtención de certificados de aptitud ocupacional, en otras palabras, se busca el capacitar y certificar a las personas en formaciones técnicas y tecnológicas[4].

De acuerdo con lo establecido en el Decreto 2020 de 2006, la educación para el trabajo y el desarrollo humano es un proceso que ayuda las personas a que desarrollen competencias laborales relacionadas con determinados campos ocupacionales referidos por el Estado colombiano y que permiten realizar una actividad económica bien sea como empleado o como emprendedor.

[3] BALTAZAR, J. (2011). Diseño e implementación de un esquema de seguridad perimetral. Para redes de datos caso práctico: dirección general del colegio ciencias y humanidades. 2016, de UNAM - México Disponible en: http://132.248.9.195/ptb2011/mayo/0669103/0669103_A1.pdf

[4] COLOMBIA. MINEDUCACION (2016). Disponible en: http://www.mineducacion.gov.co/1759/w3-article-234968.html

Teniendo como referencia lo anterior, dentro de la Educación para el Trabajo y el Desarrollo Humano se distinguen 2 clases de Programas de Formación:

Programas de Formación laboral: este tipo de programas tiene como objetivo la preparación de las personas en áreas específicas de producción y desarrollo de competencias para el sector laboral, de tal suerte que éstos tengan una rigurosidad de instrucción de seiscientas (600) horas con una formación práctica.

Programas de Formación Académica: se centra en la formación de conocimientos y habilidades en los diversos temas científicos, tecnológicos, de humanidades, arte, idiomas, entre otros. Así pues, dichos programas tienen una duración mínima de ciento sesenta (160) horas[5].

Teniendo en cuenta lo anterior, el Instituto COTEL-TUNJA es una Institución de educación para el trabajo y el desarrollo humano la cual ofrece programas de formación laboral en la ciudad de Tunja.

5.2.2. Amenaza informática. Se entiende como amenaza informática "toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio" [6]. Así pues, se deduce que una amenaza informática implica la aparición de una situación no beneficiosa a la cual se expone tanto una persona (usuario informático) como un sistema informático, teniendo como consecuencia la pérdida de un bien informático (hardware en su definición más simple como computadores o partes de los mismos), o por otro lado, la aparición de una amenaza lógica (entendiéndose todas aquellas amenazas que afecten a la información como virus informáticos, robo o pérdida información, entre otros).

5.2.2.1. Tipos de amenazas lógicas en informática. Uno de los puntos más débiles frente a la seguridad informática es la experiencia de las propias personas las cuales se exponen a diferentes riesgos en la informática ya sea por falta de preparación o simplemente por sucesos accidentales. En ese sentido, se puede clasificar algunas de las amenazas lógicas más comunes que se encuentran en informática de la siguiente forma:

[5] MINEDUCACION - COLOMBIA. (2016). Educación para el Trabajo y el Desarrollo Humano - Definicion. 2016, de MINISTERIO DE EDUCACION DE COLOMBIA Disponible en: http://www.mineducacion.gov.co/1759/w3-article-234968.html

- **Ingeniería social:** consiste en la manipulación de las personas para que revelen sus datos legítimos a través de técnicas informáticas o de persuasión.

- **Shoulder Surfing:** significa espiar por encima del hombro a una persona. Es decir, espiar lo que una persona está haciendo en un computador sin que se dé cuenta.

- **Basureo:** a través de este método lo que se busca es obtener información de un usuario a través de los restos que haya dejado en algún sistema informático, por ejemplo, una sesión abierta o elementos que haya dejado en la papelera de reciclaje de Windows.

- **Bombas lógicas**: son programas que tienen un código listo para ejecutarse al momento en que se cumpla una fecha o condición, tras lo cual empiezan implementar los códigos y acciones para los que han sido diseñados sea robo de información o daño de un sistema informático.

- **Virus**: es un programa cuyo código busca alterar el funcionamiento en un computador sin que el usuario del mismo se dé cuenta con el fin de afectar negativamente los datos almacenados en un computador, dicha acción puede ser realizada con el propósito de ocasionar daños o buscar algún tipo de beneficio económico.

- **Gusanos**: es un tipo de virus que tiene la capacidad de realizar copias de sí mismo una vez que infecta varios computadores o dispositivos.

- **Caballos de Troya**: son programas o archivos que se muestran al usuario como si fueran legítimos o benignos, no obstante, llevan un código malicioso con el objetivo infectar o causar daño.

- **Spyware**: son programas espía que se encargan de recopilar la información sobre una persona para luego enviarla al atacante el cual hará uso económico de esta.

- **Phishing**: consiste en la obtención de información de una persona a través de un programa, código malicioso o formulario, el cual se hace pasar por un medio legítimo; un ejemplo de ello es el envío de correos electrónicos como si fueran una fuente confiable o el uso de páginas web falsificadas.

- **Técnicas salami**: consiste en el robo de pequeñas cantidades de cuentas de dinero bancarias haciéndolo de forma sistematizada, generalmente los atacantes que realizan esta labor son empleados de las mismas entidades bancarias.

- **Escaneo de puertos:** es un escaneo se realiza a algunos de los principales puertos de un computador desde otro para comprobar si están abiertos, de ser así se intentan realizar ataques a través de los mismos para poder acceder al computador de la víctima y obtener información de la misma.

5.2.2.2. Amenazas del personal interno. Como lo señala A. Gómez Vieites "se debe tener en cuenta el papel desempeñado por algunos empleados en muchos de los ataques e incidentes de seguridad informática, ya sea de forma voluntaria o involuntaria. Así se llega a considerar el papel de los empleados que actúan como "fisgones" en la red informática de su organización, los usuarios incautos o despistados, o los empleados descontentos o desleales que pretenden causar algún daño a la organización. Por este motivo, conviene reforzar la seguridad tanto en relación con el personal interno ("insiders") como con los usuarios externos del sistema informático ("outsiders")"[7]. Teniendo como referencia lo anterior se puede apreciar como la seguridad no sólo implica la protección del perímetro de un sistema informático en una organización sino también se debe garantizar y vigilar la operación del mismo frente a los usuarios internos ya que ellos son un principal foco de generación de problemas de seguridad.

5.2.3. Conceptos de Hardening. Antes de avanzar en el concepto de hardening vale aclarar que las palabras hardening y bastionamiento son sinónimos en el tema de seguridad informática ya que ambas significan el aseguramiento de un sistema informático (el cual puede estar compuesto de hardware o software). Así pues la palabra bastionar procede de la palabra abastionar definida por la Real Academia Española como el proceso de fortalecer con bastiones, lo cual deviene históricamente de las fortificaciones de los castillos medievales que se llamaban bastiones y que cubrían áreas críticas de defensa en caso de invasión[8].

[7] A. Gómez Vieites. (2014). La lucha contra el ciberterrorismo y los ataques informáticos. 2016, de edisa.com Disponible en: http://www.edisa.com/wp-content/uploads/2014/08/La_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf
[8] Wikipedia. (2016). Bastion host. 2016, de Wikipedia Disponible en: https://es.wikipedia.org/wiki/Bastion_host

De esta manera, el bastionado de sistemas o hardening, tal como lo define la empresa Tarlogic, “es 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”[9]. Como es de aclarar, el bastionamiento puede abarcar desde medidas en software dependiendo del sistema operativo que manejen las estaciones de trabajo (entre ellas destacarían antivirus, políticas de grupo, permisos de cuentas, etc) así como también medidas en hardware que ayudan a proteger la periferia del sistema y su red en términos físicos (como ejemplo se tendrían firewalls, implementación de DMZ, IDS, honeynets, routers, UPS, entre otros).

Otra palabra muy utilizada y que tampoco aparece en la RAE, pero que es de uso extendido para hardening es "securizar”, incluso alguna veces se usa la palabra "hardenizar" que deriva claramente del inglés”[10].

5.2.4. Bastionado de un sistema informático. Un sistema informático requiere de un bastionado para brindar una mayor seguridad extra fuera de las medidas que por defecto implemente, tal como lo detalla Rodríguez, Lorenzo “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”.[11] Así pues, el hardening hace difícil la labor de un atacante informático, toda vez que entorpece su accionar y permite ganar tiempo a la organización para poder minimizar las consecuencias e implementar nuevas medidas si es el caso con el fin de proteger los activos informáticos.

A. Gómez Vieites identifica aquellos perjuicios a los que se enfrente una empresa en caso de un ataque informático como son:

➢ “Horas de trabajo invertidas en las reparaciones y reconfiguración de los equipos y redes.

[9] TARLOGIC. (2016). Bastionado de sistemas (hardening). 2016, de Tarlogic Disponible en: https://www.tarlogic.com/servicios/bastionado-de-sistemas-hardening/

[10] MARTÍNEZ, Lorenzo. (2009). ¿Nos expresamos correctamente? 2016, de securitybydefault.com Disponible en: http://www.securitybydefault.com/2009/11/nos-expresamos-correctamente.html

[11] MARTÍNEZ, Lorenzo (2015). La importancia del bastionado de sistemas. Disponible en: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/importancia_bastionado_sistemas

➢ Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos: coste de oportunidad por no poder utilizar estos recursos.

➢ Robo de información confidencial y su posible revelación a terceros no autorizados: fórmulas, diseños de productos, estrategias comerciales, programas informáticos.

➢ Filtración de datos personales de usuarios registrados en el sistema: empleados, clientes, proveedores, contactos comerciales…"[12]

De igual manera, hay que manifestar que la implementación de medidas tecnológicas de seguridad han de ser idóneas y bien implementadas para que no impliquen un desperdicio financiero en una organización, tal como lo referencia Ana Carrillo: "Se debe tener en cuenta que las implementaciones tecnológicas invertidas en cada empresa son de alto costo y lo que ellas buscan es que las personas agilicen cada una de sus transacciones de manera oportuna y que sean utilizadas adecuadamente ya que si las mismas son inutilizadas generarían un deterioro al patrimonio de la empresa, por ende es necesario que las implementaciones tecnológicas lleven consigo la carga de la seguridad de la información con el fin de lograr prestar un buen servicio a los clientes y generar en ellos la confianza necesaria para seguir utilizándolas de lo contrario toda la inversión se perdería[13].

5.2.5. Hardening en software. La empresa grammatech señala respecto del hardening en software que este "se realiza a través de tres técnicas básicas: análisis de la vulnerabilidades, parches y monitoreo de software"[14]. No obstante, el proceso de hardening implica la utilización de una mayor variedad de técnicas y medidas algunas de ellas nuevas o no documentadas. En ese orden de ideas, la empresa SyR propone una serie de acciones necesarias para poder hacer el sistema más seguro:

- Eliminando software innecesario u obsoleto
- Eliminando servicios innecesarios u obsoletos
- Eliminando usuarios que ya no trabajen en la empresa.

[12] A. Gómez Vieites. (2014). La lucha contra el ciberterrorismo y los ataques informáticos. 2016, de edisa.com Disponible en: http://www.edisa.com/wp-content/uploads/2014/08/La_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

[13] Ana Rodríguez. (2014), análisis y diagnóstico de la seguridad informática de Indeportes Boyacá. 2106, de UNAD Disponible en: http://repository.unad.edu.co/bitstream/10596/2692/5/53070244.pdf

[14] Grammatech. (2016). Software Hardening. 2016, de grammatech.com. Disponible en: https://www.grammatech.com/software-hardening

- Cerrando puertos innecesarios
- Upgrade del firmware
- Instalación segura del sistema operativo
- Configuración adecuada de servicios de actualización automática
- Instalación y configuración adecuada de programas de seguridad (Antivirus, Antispyware, Antispam…)
- Políticas de contraseñas robustas[15]

5.2.5.1. Hardening en Windows. Es de resaltar que en un ambiente Windows el aseguramiento de las estaciones de trabajo es una de las labores más esenciales y más profundas, teniendo en cuenta que Windows es uno de los sistemas operativos más atacado de este momento después de Android. En ese sentido, frente la aplicación de hardening en este ambiente informático se resalta una amplia disponibilidad de técnicas, procesos y herramientas para aplicar. Entre ellas destacan:

- Actualizaciones de Windows: es la medida más recomendada ya que ayuda no solo a corregir errores de programación, sino también a solucionar backdoors e implementa parches de seguridad frente a las amenazas que surgen a diario.

- Antivirus: El uso de software antivirus supone una medida importante en lo que se refiere a un ambiente Windows ya que de llegarse a presentar una infección viral esta puede ser eliminada o contrarrestada, no obstante, la efectividad de ello depende de la robustez del antivirus, así como de la coincidencia del virus con la base de datos que implemente.

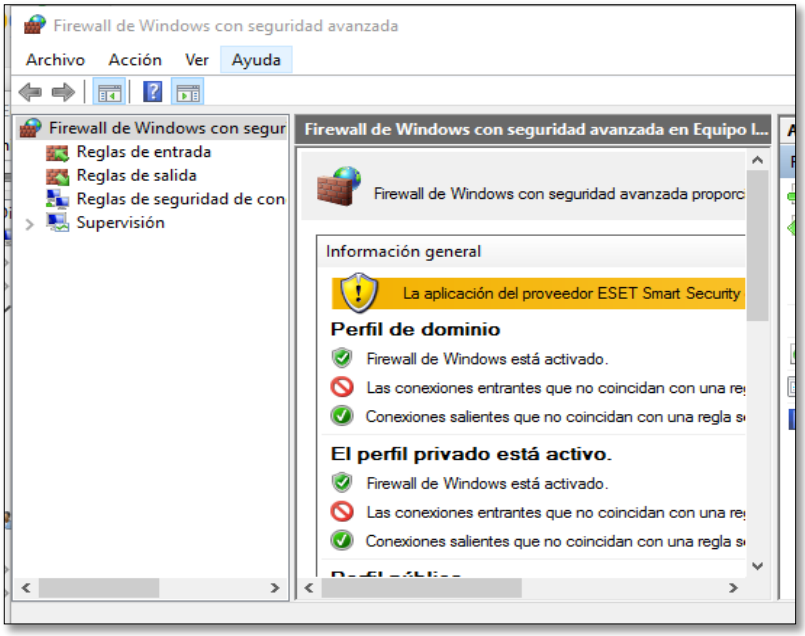
- Cuentas de usuario: es una herramienta bastante importante y poco usada de Windows ya que permite establecer qué usuarios pueden realizar instalaciones o modificaciones del sistema operativo dejando a un lado aquellos que sólo deban hacer uso de las aplicaciones.

- Firewall: “es un sistema que permite proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red (expresamente de Internet). El firewall es un sistema que permite filtrar los

[15] Seguridad SyR. (2016). Bastionado de sistemas y servidores. 2016, de Seguridad SyR. Disponible en: https://seguridad.syr.es/servicios-seguridad-informatica/bastionado-de-sistemas-y-servidores

paquetes de datos que andan por la red”[16]. En este caso, el firewall de Windows hace uso de una colección de restricciones personalizables denominadas reglas las cuales puede ser configuradas para permitir o denegar conexiones de red, así como de programas, a la vez que también permite el cerrar puertos de comunicaciones.

Figura 1. Firewall de Windows 10.



Fuente: El autor

5.2.5.2. Hardening en Linux. De igual suerte es de señalar que Linux en sí mismo ofrece una protección ya que no es un sistema operativo tan atacado y su modo de uso varia respecto de Windows al no otorgar permisos de instalación o modificación al libre albedrio como si lo hace Windows u otras plataformas. Linux puede convertirse también en uno de los principales bastiones de protección en el caso de implementar una defensa a profundidad, sin embargo, es un sistema operativo que se pueda robustecer con medidas en hardening, siendo así el sitio Tecmint destaca las siguientes[17]:

[16] Informática-hoy. (2016). Que es un Firewall y cómo funciona. 2016, de informatica-hoy. Disponible en: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Firewall-y-como-funciona.php
[17] Ravi Saive. (2013). 25 Hardening Security Tips for Linux Servers. 2016, de tecmint. Disponible en: http://www.tecmint.com/linux-server-hardening-security-tips/

- Sistema de Seguridad Física: desactivar el arranque de dispositivos externos en el BIOS y proteger el GRUB con contraseña para restringir el acceso al sistema.

- Particiones: usar diferentes particiones para obtener una mayor seguridad de los datos en caso de que ocurra algún desastre. Para este caso es usual darles una partición distinta a los archivos del usuario, los del sistema operativo, los de la carpeta intercambio o swap, entre otros.

- Verificar los puertos de escucha de red: Con ayuda del comando' netstat ' se puede ver todos los puertos abiertos y programas que hagan uso de los mismo, igualmente usando chkconfig se puede desactivar aquellos los servicios de red no deseados del sistema con lo cual se reduce la superficie de ataque en caso de vulneración a través de puertos.

- Uso de Secure Shell (SSH): este protocolo de seguridad se puede usar para la encriptación de mensajes en la consola de comandos de Linux (Shell).

- Desactivar la detección de memorias USB: con la creación de un archivo que contenga el comando /etc/modprobe.d/no-usb , se restringirá el uso o detección de dispositivos USB de almacenamiento.

De igual manera se puede realizar instalación de programas de hardening en Linux como Grsecurity, el cual establece controles del sistema Linux a través de un sistema a modo de parche del KernelM entre sus funciones destacan la prevención de la ejecución del código arbitrario, control de ejecución de las tareas en el stack, control de las actividades de los usuarios, entre otros[18].

5.2.6. Hardening en cuanto a hardware. Igualmente, no sólo se puede hacer referencia a la aplicación de métodos o procesos de aseguramiento específicamente en software, también se puede hablar de medidas de hardware las cuales pueden ir desde dispositivos físicos firewalls o IDS, o incluso hasta implementar medidas aún más robustas como sistema de reconocimiento de biométricos.

[18] DragoN. (2008). Que es el Hardening Linux con grsecurity. 2016, de dragonjar.org. Disponible en: http://www.dragonjar.org/hardening-linux-con-grsecurity.xhtml

5.2.6.1. IDS – Sistema de detección de intrusos. Un IDS (Intrusion Detection System) es una herramienta de seguridad, que se encarga de monitorizar los sucesos que resultan en un sistema informático en busca de intentos de intrusión[19]. Hablando en el caso de hardware, se encuentran dispositivos de detección de intrusos de venta al público ofrecidos por la empresa Cisco y dentro de los que destacan productos como IDS 4215 Sensor[20], Catalyst 6500 (IDSM-2)[21] o FirePOWER 8000 [22]. Éstos dispositivos además de ofrecer las labores IDS, también permiten contrarrestar o moderar ataques de DDOS, así como un buen manejo de ancho de banda para trabajar más rápido en una red de comunicación informática.

5.2.6.2. Dispositivos firewalls. CISCO define un firewall como "un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad, esto ayuda a establecer una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. Un firewall puede ser hardware, software o ambos" [23]. Teniendo presente el concepto anterior, un firewall puede estar constituido por software o puede ser un dispositivo físico siendo este último más efectivo ya que su labor de seguridad es especifica en tanto que el de software por lo general viene de forma predeterminada en cada sistema operativo.

A manera de ejemplo se pueden citar dispositivos firewalls físicos de la línea comercial de la empresa Watchguard como son WatchGuard Firebox M4600 & M5600, WatchGuard Firebox M400 & M500, WatchGuard Firebox M440[24]. Estos dispositivos además de los procesos propios de un firewall permiten ser posicionados en cualquier punto del perímetro de una red de comunicación y manejan altas velocidades de ancho de banda.

---

[19] Garzon Padilla, G. (2015). Propuesta para la implementación de un sistema de detección de intrusos (IDS) en la Dirección General Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC "pidsinpec". Disponible en:http://hdl.handle.net/10596/3494

[20] CISCO. (2016). Cisco IDS 4215 Sensor. 2016, de CISCO. Disponible en: http://www.cisco.com/c/en/us/support/security/ids-4215-sensor/model.html

[21] CISCO. (2016). Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Module. 2016, de CISCO Disponible en: http://www.cisco.com/c/en/us/products/interfaces-modules/catalyst-6500-series-intrusion-detection-system-idsm-2-services-module/index.html

[22] CISCO. (2016). Cisco FirePOWER 8000 Series Appliances. 2016, de CISCO. Disponible en: http://www.cisco.com/c/en/us/products/security/firepower-8000-series-appliances/index.html

[23] CISCO. (2016). ¿Qué es un firewall?. 2016, de CISCO. Disponible en: http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

[24] Watchguard. (2016). Firewall de nueva generación (NGFW). 2016, de watchguard.com Disponible en: http://www.watchguard.com/es/wgrd-international/products/ngfw/overview

5.3. MARCO CONTEXTUAL

La actividad comercial de la institución COTEL de Tunja gira alrededor de su figura como Institución de Educación Para el Trabajo y el Desarrollo Humano, la cual se centra en la formación y capacitación de personas en programas de Formación laboral como son:

- Ajuste y reparación de equipos electrónicos
- Auxiliar de archivo y registro
- Belleza integral
- Cocina
- Contabilidad y finanzas
- Diseño grafico
- Mecánica de motores de combustión interna
- Recepción hotelera y turística
- Salud ambiental
- Secretariado auxiliar contable
- Seguridad ocupacional
- Sistemas

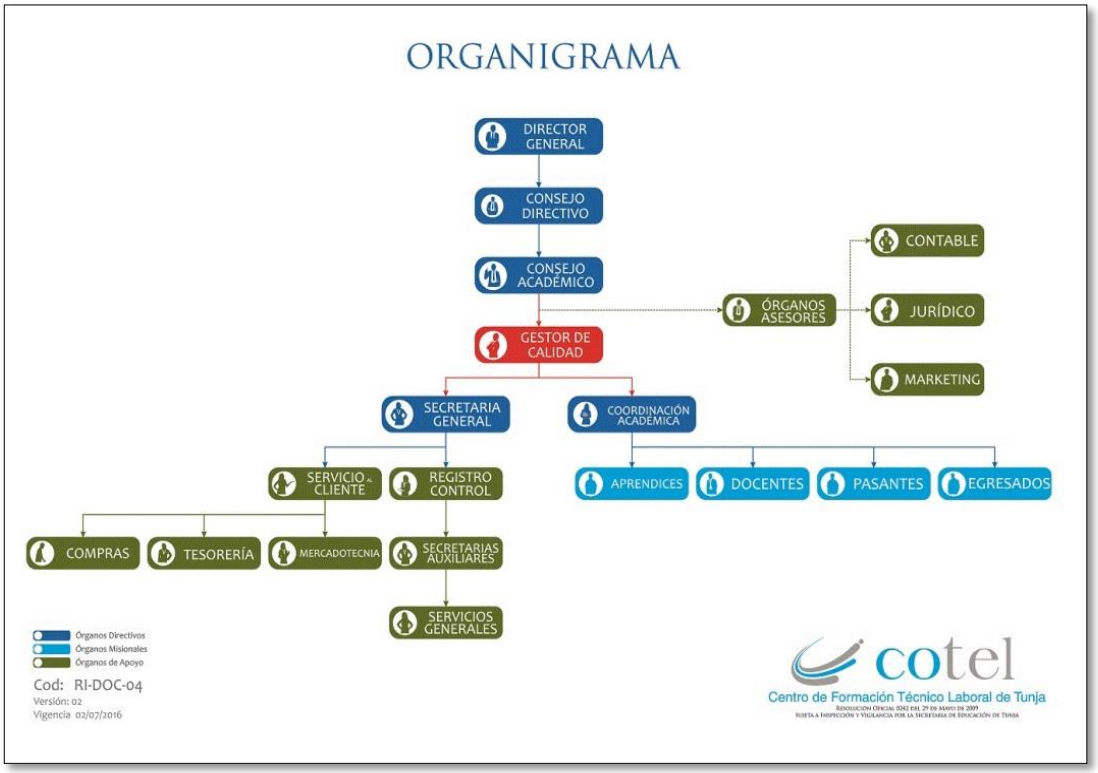
5.3.1. Reseña histórica COTEL-TUNJA. "*El Centro De Formación Técnico Laboral De Tunja "COTEL" es una institución de educación para el trabajo y el desarrollo humano fundada el 15 de Marzo del año 2004, como una entidad privada sin ánimo de lucro, autorizada por la Secretaria de Educación Departamental de Boyacá y que extiende sus servicios a la comunidad académica, sus colaboradores y la comunidad en general, de acuerdo a la normatividad legal vigente para la prestación del servicio educativo a través de Resolución No. 0399 del 15 de Marzo de 2004 por la Secretaria de Educación Departamental de Boyacá mediante la cual se crea COTEL y luego a través de la Resolución 0242 de Mayo 29 de 2009 que concedió licencia de funcionamiento a la Institución.*

MISION: formar ciudadanos competentes, con excelencia académica y pertinencia laboral bajo la normatividad vigente que responda a las necesidades del entorno.

VISION: ser la institución líder en procesos educativos basados en competencias laborales con reconocimiento a nivel departamental y nacional bajo un sistema de gestión de calidad que cumpla los estándares normativos vigentes" [25].

5.3.2. Organigrama organizacional COTEL-TUNJA

Figura 2. Organigrama COTEL-TUNJA



Fuente: Coordinación SGC COTEL

5.3.3. Sistemas de gestión de calidad en COTEL-TUNJA. El instituto COTEL de Tunja, en aras de mejorar la atención a la comunidad estudiantil y ciudadanía en general, entro en un proceso de mejora administrativa cuyos frutos fueron las certificaciones alcanzadas a través de 4 sistemas de gestión de calidad:

ISO 9001: Sistema de gestión de calidad que centra en todos los elementos de administración de calidad con los que una empresa debe contar para tener un

[25] COTEL - Tunja (2014). Manual de convivencia Acuerdo 01 del 24 de junio de 2014. (2016)

sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios[26].

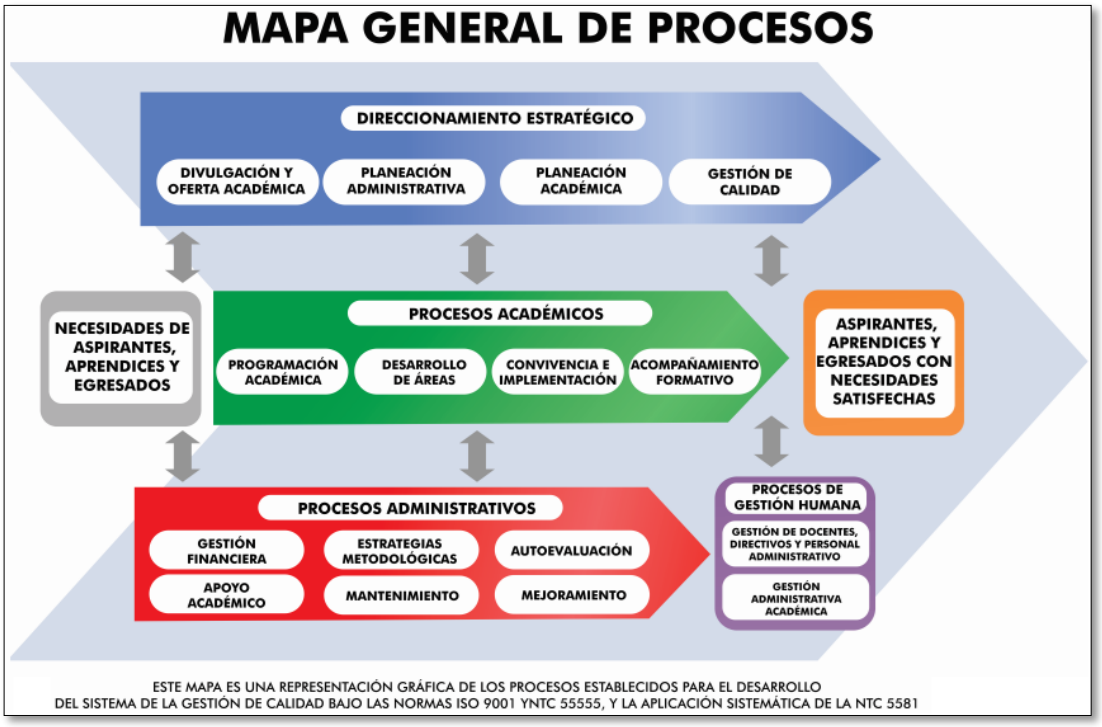
NTC 5555: Sistema de gestión de calidad para instituciones de formación para el trabajo y desarrollo humano

NTC 5581: Especifica los requisitos de calidad que deben tener los programas de formación para el trabajo y desarrollo humano

NTC 5666: Establece los requisitos de calidad de los programas de formación para el trabajo en el sector de sistemas informáticos

Dichos sistemas de gestión han permitido al instituto posicionarse como la entidad privada de educación líder en el ofrecimiento de programas de formación laboral a nivel de Boyacá cumpliendo con el objetivo visional establecido en el año 2010 y que fue igualmente certificado por el ente de certificación Cotecna (empresa certificadora de ISO 9001 a nivel Colombia).

Figura 3. Mapa de procesos ISO 9001 y NTC 5555 en COTEL



Fuente: Coordinación SGC COTEL

[26] Normas9000. (2016). ¿Qué es ISO 9001:2008? Disponible en: http://www.normas9000.com/que-es-iso-9000.html

5.3.4. Activos informáticos de COTEL-TUNJA. El inventario de los activos del instituto se hizo tomando como referencia la metodología Magerit[27] para este efecto y como se detalla a continuación:

Tabla 1. Inventario Activos informáticos COTEL-TUNJA

TIPOS DE ACTIVOS	DESCRIPCION
ACTIVO DE INFORMACION	Bases de Datos manejadas en hojas de Excel en formato .xlsx, archivos de registro de información de estudiantes y empleados en archivos Word .docx, texto plano .txt y .pdf. Archivos de publicidad y registro fotográfico en formatos de imagen .jpeg .bmp .png. Archivos de Diseño gráfico en formatos .cdr .psd.
SOFTWARE DE APLICACIÓN	Windows 7 versiones Professional y Ultimate en arquitecturas x86-x64 Windows 10 home single language Paquete ofimático Microsoft Office 2010 Paquete ofimático Microsoft Office 2013 Corel draw x7 Suite de Adobe cs5 3dmax Virtual Box Antivirus: Microsoft Security Essentials Software de contabilidad SIIGO versión 8 gráfica y versión 1999 versión consola Página de internet: www.cotel.edu.co. (La página del instituto es publicitaria, por tanto, no maneja bases de datos ni campus virtual. Hosting: interactiva.net.co. Plan básico sin acceso a acceso a cpanel, ni bases de datos, ni correo corporativo). El instituto no maneja ningún otro aplicativo por fuera de los mencionados, sea el caso de aplicaciones de gestión, campus o biblioteca virtual u otras.

[27] UNAD. (2016). 233003 Sistema de gestión de la seguridad de la información sgsi - Inventario de Activos. 2016, de UNAD. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321_paso_1_inventario_de_activos.html

Tabla 1. (Continuación)

HARDWARE	• 91 Computadores de escritorio (estaciones de trabajo) Características estaciones de trabajo (computadores): Mother boards: Intel g41rq - Intel dg55rq Memoria RAM de 4,00 GB Procesador INTEL CORE I3 Distribución física de los computadores: 84 computadores están destinados a 6 aulas de computación para procesos de enseñanza. 7 computadores restantes se destinan para labores administrativas Distribución de sistemas operativos en los computadores: 84 computadores presentan Windows 7 X64 en versiones home Premium y Profesional 7 computadores se encuentran instalados en Windows 10 x64 version home single language. • 3 impresoras (HP 1102 – HP 1102w – Epson l255)
RED	2 Router D-LINK cada uno con un canal de 4 MB de ancho de banda, ambos contratados con el IPS Movistar 12 Switches Q-link
EQUIPAMIENTO AUXILIAR	35 estabilizadores (de 600 y 1000W)
INSTALACION	Red de cableado sin estructurar Cableado en UTP categoría 5e con conectores RJ45 18 puntos de red identificados en 14 salas Cableado eléctrico trifásico
SERVICIOS	Servicios públicos básicos, internet (2 canales de 4 mb cada uno), celular.
PERSONAL	7 empleados administrativos (3 secretarias, 1 rector, 1 coordinadora, 1 director de pasantías, 1 asesor jurídico) 4 empleados departamento de sistemas (1 técnico de sistemas, 3 auxiliares pasantes de sistemas) 54 instructores (que imparten catedra en las diferentes carreras técnicas) Total: empleados: 65 Usuarios adicionales: 600 estudiantes

Fuente: El autor

5.4. MARCO CONCEPTUAL

Addware: software que automáticamente añade o muestra publicidad junto a la instalación de otro programa o en una página web, no es nocivo, pero si molesto ya que genera ventanas flotantes esto hace que algunas veces se clasifique como un malware.

Amenaza informática: se define como un elemento o acción capaz de atentar contra la seguridad de un sistema informático en forma de robo, destrucción, divulgación o alteración de datos [28].

Antivirus: es un programa de seguridad que ayuda a proteger un equipo o dispositivo informático frente a ataques virales u otro tipo de invasores no deseados; dicha labor la realiza a través de un monitoreo en tiempo real teniendo como referencia una base de virus la cual es frecuentemente actualizada [29].

Backdoors: es un programa malicioso creado por un atacante para obtener acceso remoto a un dispositivo informático con el fin de controlarlo sin conocimiento por parte del usuario o propietario del mismo[30].

Dirección MAC: es un identificador de 48 bits que corresponden de forma universal a una única tarjeta o periférico de red bien sea de un computador o un dispositivo móvil.

DMZ: (Zona desmilitarizada) es una zona que se crea por fuera del perímetro de una red de computadores para protegerla. Se ubica entre la red interna de una organización y una externa (internet) con el fin de que aquellos que deseen hacer uso de los servicios de la organización a través de Internet sólo puedan acceder a una parte de la red (en este caso la DMZ) y no a toda la red entera. Así pues, la DMZ puede estar compuesta de servidores web, de correo o computadores de uso para el público en general.

---

[28] Glosario de Seguridad 101. Symantec. Disponible en:https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[29] ibídem

[30] Pergaminovirtual. (2015). Definición de Backdoor. 2016, de pergaminovirtual.com. Disponible en: http://www.pergaminovirtual.com.ar/definicion/Backdoor.html

Estación de trabajo: es un computador generalmente de uso personal que está unido a una red de computadores y cuyo objetivo es maximizar el trabajo que se realiza en estos [31].

Exploit: es un código malicioso el cual busca deficiencias o vulnerabilidades de un sistema con el fin de destruirlo, inhabilitarlo o acceder al mismo para obtener información de forma ilegal [32].

Filtrado MAC: Este proceso se realiza para restringir el acceso a la red a determinados dispositivos y permitírselo sólo a aquellos a los que se les haya dado una autorización específica teniendo en cuenta su dirección MAC, generalmente es usado en la seguridad de redes Wi-Fi.
Firewall: es un software o hardware que identifica y bloquea intentos de intrusión o comunicación hacia fuera de una red informática o limita el acceso a contenidos de los usuarios de la misma.

Hardening: es el proceso de protección de un sistema o conjunto de sistemas informáticos (bien sea hardware o software) mediante la aplicación de configuraciones de seguridad específicas a modo de barrera sucesivas con el fin de prevenir y ralentizar ataques informáticos[33].

Honeynet: es una red trampa creada con vulnerabilidades intencionales y cuyo propósito es invitar a que sea atacada, por lo que las actividades y métodos de un atacante puede ser estudiados y utilizados para mejorar la seguridad de una red generando planes de acción frente a ellos sin necesidad de comprometer la red de una organización [34].

Keylogger: es un programa que al ser instalado en un computador captura las pulsaciones que se hayan hecho en el teclado de un pc (texto que se haya escrito), crea un registro de ello y se lo envía al atacante.

Linux: sistema operativo de libre distribución basado en Unix, también conocido como GNU/Linux ya que deriva del proyecto GNU. Al ser su código abierto, este

[31] Kelly Sundstrom. (2014). ¿Qué es una estación de trabajo de computadora? 2016, de ehowenespanol.com Disponible en: http://www.ehowenespanol.com/estacion-computadora-hechos_400522/
[32] Seguridadpc.net. (2016). Concepto de exploit. 2016, de seguridadpc.net. Disponible en: http://www.seguridadpc.net/exploit.htm
[33] Techopedia. (2016). Hardening. 2016, de techopedia.com. Disponible en: https://www.techopedia.com/definition/24833/hardening
[34] Limberth Torrez. (2010). ¿Qué es Honeynet?. 2016, de aiturrih.blogspot.com. Disponible en: http://aiturrih.blogspot.com.co/2010/11/que-es-honeynet.html

puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL u otras serie de licencias libres[35] .

Linux – distribución: una distribución Linux es una versión que está basada en el núcleo Linux y que incorpora ciertos paquetes de software y programación enfocada a las necesidades de un grupo específico de usuarios[36].

Patching o parcheo: es el proceso mediante el cual se actualiza o cambia un programa específico; esto con el fin de solucionar problemas o mejorar el desempeño; siendo así que existen parches de depuración, de seguridad y de actualización[37]
Seguridad informática: es el área informática que se centra en la protección de un determinado sistema de computación en lo que tiene que ver con su funcionamiento e información contenida en el mismo [38].

Sniffer: es un programa utilizado en redes informáticas que se usa para analizar y controlar el tráfico trasmitido en una red o redes[39].

TAAC (software): un programa TAAC (Técnicas de Auditoría con Ayuda de Computadora) es aquel que incluye distintos tipos de herramientas y técnicas de auditoria por computadora con el fin de dar información detallada acerca de la conformación en software y hardware de un sistema informático al que se esté aplicando[40].

Vulnerabilidad informática: se comprende como un factor de riesgo interno en el cual un sistema informático es susceptible de ser atacado o comprometido debido a las debilidades que presente el mismo[41].

---

[35] Wikipedia. (2016). GNU/Linux. 2016, de Wikipedia.org Disponible en: https://es.wikipedia.org/wiki/GNU/Linux
[36] Wikipedia. (2016). Distribución Linux. 2016, de Wikipedia.org. Disponible en: https://es.wikipedia.org/wiki/Distribuci%C3%B3n_Linux
[37] Quees.la. (2016). ¿Qué es parchear?. 2016, de Quees.la Disponible en: http://quees.la/parchear/
[38] Definicionabc. (2016). Definición de Seguridad informática. 2016, de definicionabc.com. Disponible en: http://www.definicionabc.com/tecnologia/seguridad-informatica.php
[39] Culturacion. (2016). ¿Qué es un sniffer?. 2016, de culturacion.com. Disponible en: http://culturacion.com/que-es-un-sniffer/
[40] Auditoria de sistemas. (2012). Técnicas de auditoria asistidas por computadoras. 2016, de auditoriadesistemascontaduriaucc. Disponible en: http://auditoriadesistemascontaduriaucc.blogspot.com.co/2012/06/tecnicas-de-auditoria-asistidas-por.html
[41] UNAD. (2016). Lección 1: Conceptos de Vulnerabilidad, Riesgo y Amenaza. 2016, de UNAD. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

WLAN: (Red de área local inalámbrica) es una red que utiliza las ondas de radio para transmitir datos y permite conectar dispositivos a la misma permitiéndoles acceso a Internet y a su red de computadores [42]. Coloquialmente conocida como señal Wi-Fi.

WPE: estándar de seguridad para redes Wi-Fi que permite cifrar la información que se transmite.

WPA: estándar de seguridad para redes Wi-Fi mejorado a partir del WEP incluyendo fortalezas como el TKIP (Temporal Key Integrity Protocol [43].

5.5. MARCO LEGAL

Se tendrá como base la normatividad colombiana vigente para el desarrollo, ejecución y protección del estudio.

5.5.1. Ley 599 de 2000. Código Penal de Colombia. En lo que se refiere a código penal se verifican los artículos que consagran la protección a los derechos de autor[44].

Artículo 270. Violación a los derechos morales de autor. [Penas aumentadas por el artículo 14 de la ley 890 de 2004] Incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de veinte seis puntos sesenta y seis (26.66) a trescientos (300) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.

2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado,

[42] CISCO. (2016). WLAN. 2016, de CISCO. Disponible en: http://www.cisco.com/c/es_es/solutions/mobility/wlan.html
[43] Angel Gutierrez. (2015). WEP o WPA para proteger tu red Wi-Fi. 2016, de windowsespanol. Disponible en: http://windowsespanol.about.com/od/RedesYDispositivos/a/Wep-O-Wpa-Para-Proteger-Tu-Red-Wi-Fi.htm
[44] República de Colombia. (2000). Ley 599 de 2000 – Código penal. 2016, de cerlalc.org. Disponible en: http://www.cerlalc.org/derechoenlinea/dar/leyes_reglamentos/Colombia/Ley_599.htm

modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. [Modificado por el artículo 2 de la ley 1032 de 2006.] Incurrirá en prisión de cuatro (4) a ocho (8) años y multa de veintiséis puntos sesenta y seis (26.66) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la ley, sin autorización previa y expresa del titular de los derechos correspondientes:

Por cualquier medio o procedimiento, reproduzca una obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o, quien transporte, almacene, conserve, distribuya, importe, exporte, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones. Represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, video gramas, obras cinematográficas, o cualquier otra obra de carácter literario o artístico.

Alquile o, de cualquier otro modo, comercialice fonogramas, video gramas, programas de ordenador o soportes lógicos u obras cinematográficas.
Fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales.

Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título.

Retransmita, fije, reproduzca o, por cualquier medio sonoro o audiovisual, divulgue las emisiones de los organismos de radiodifusión.

Recepciones, difunda o distribuya por cualquier medio las emisiones de la televisión por suscripción.

5.5.2. Ley 603 de 2000. Derechos de autor. Por la cual se modifica el artículo 47 de la Ley 222 de 1995, esta ley hace referencia a la protección de los derechos de autor en Colombia. Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado, dicha ley faculta a la Unidad Administrativa Especial Dirección Nacional de Derecho Autor para ejercer el control y registro de los derechos de autor.

5.5.3. Ley 1273 de 2009. Derechos de autor. De La Protección De La Información Y De Los Datos. Se refiera a delitos informáticos y la protección de la información y de los datos fue creada en Colombia el 5 de enero de 2009 por el congreso de la república la cual modifico modifica el código penal creando un nuevo mecanismo legal para sancionar todo comportamiento ilícito frente a la comisión de los delitos informáticos en el país, así como la protección de datos personales.

Esta ley creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

Articulo 269 A: trata acerca del acceso abusivo a un sistema informático en donde tipifica el Acceder a un equipo de forma abusiva o sistema con el fin de extraer información.

Articulo 269 C: trata acerca de interceptación ilícita de datos informáticos donde penaliza a aquellos que Obstruyen datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático.

Articulo 269 E: trata acerca de cuándo se emplea algún software con el fin de sacar un provecho propio o generar un daño a un equipo de cómputo.

Articulo 269 G: trata acerca de la suplantación de sitios web para capturar datos personales, en el sentido de crear una página similar a la de una entidad o enviar correos engañosos, con el fin de obtener información personal, claves bancarias o demás datos de importancia económica.

6. MARCO METODOLÓGICO

6.1. TIPO DE INVESTIGACION

Esta investigación seguirá una estructura basada en un estudio **descriptivo**[45], ya que se buscará identificar antecedentes y referencias respecto del tema seleccionado como objeto de estudio (hardening), en ese sentido, se buscará la información en fuentes seleccionadas como como trabajos de investigación realizados en torno al tema tratado en el proyecto; de igual forma serán consultados ensayos, artículo científico y revistas especializadas que se relacionen con el tema. Mediante un estudio descriptivo se establecerá características del tema de investigación, a la vez que permite analizar la información obtenida y dar con resultados claros frente a los objetivos definidos inicialmente en esta propuesta, esto beneficia especialmente el procesamiento de la información recopilada y la organización para consolidar la propuesta de hardening para el instituto COTEL-TUNJA que será el eje central de resultado del presente trabajo.

6.2. DISEÑO METODOLÓGICO

Los métodos a utilizar en esta investigación serán **análisis** y **síntesis**[46]. Análisis, porque se fragmentará el problema central de la investigación en problemas específicos de tal modo que se pudo identificar claramente cada aspecto indagado, así se podrá iniciar el estudio por las partes más específicas para luego llegar a una explicación general del problema. Síntesis, porque se relacionará todos los componentes del problema y se crearon explicaciones a partir de su estudio.

6.3. FUENTES DE INFORMACIÓN

6.3.1. Fuentes primarias. Las fuentes primarias para este estudio serán aquellos contenidos referentes al hardening que se encuentren en tesis, monografías, así como artículos de internet.

[45] MENDEZ, Carlos, Metodología, Diseño y Desarrollo del Proceso de Investigación. Colombia. 2001. p.136
[46] MENDEZ, Carlos, Metodología, Diseño y Desarrollo del Proceso de Investigación. Colombia. 2001. p.146-147.

6.4. POBLACIÓN

Para este proyecto la población estará constituida por los estudiantes, docentes y personal administrativo del instituto COTEL- Tunja, ubicado en la ciudad de Tunja capital de departamento de Boyacá, con dirección comercial Pasaje de Vargas 88-16.

6.5. METODOLOGÍA DE DESARROLLO

Con el fin de alcanzar los objetivos de este proyecto se ha establecido una serie de actividades a desarrollar:

Tabla 2. Metodología de desarrollo.

OBJETIVO	ACTIVIDADES
Objetivo 1: Indagar en diferentes fuentes de información acerca del proceso de hardening señalando la aplicabilidad, ventajas, estrategias y técnicas del mismo, a la vez que se reconocerá la importancia del concepto de defensa en profundidad respecto del modelo promovido por Microsoft, las capas que lo componen y su modo de aplicabilidad.	✓ Recolección de información acerca de los conceptos teóricos de hardening planteados en este objetivo. ✓ Identificar el uso del modelo de defensa en profundidad y su uso. ✓ Determinar la aplicabilidad del modelo de defensa en profundidad de acuerdo al modelo promovido por Microsoft.
Objetivo 2: Estudiar herramientas y medidas de hardening en estaciones de trabajo tipo Windows describiendo el uso de Snort como IDS, WinAudit como software TAAC, software Reboot Restore , bloqueo a través del	✓ Reconocer el uso Snort como IDS (sistema de detección de intrusos) en una plataforma Windows. ✓ Evidenciar la importancia y uso de WinAudit como software TAAC para verificar la seguridad de una estación de trabajo en Windows.

Tabla 2. (Continuación)

hosts y aplicación políticas de seguridad en Windows y Windows server.	✓ Indagar acerca de software tipo Reboot Restore (congelador). Identificar ventajas y desventajas de su implementación. Resaltar las distintas opciones en el mercado de este software y como se puede aplicar. ✓ Demostrar como bloquear el acceso a sitios web en una organización a través de la configuración del archivo hosts en estaciones de trabajo que usen Windows ✓ Diferenciar el uso y aplicación Políticas de seguridad en Windows y Windows server. Aplicación de políticas de grupo y local (GPO y GPL).
Objetivo 3: Identificar herramientas y medidas de hardening para estaciones de trabajo basadas en Linux a través del reconocimiento de características de Lynis y opciones de bastionado en Linux Ubuntu.	✓ Reconocer la aplicabilidad de Lynis enfocada a hardening indicando las características que presenta para tal fin. ✓ Identificar herramientas de hardening en software que se pueden implementar en una distribución Linux Ubuntu versión 16.04 desktop
Objetivo 4: Presentar a través de un informe, las respectivas recomendaciones para mejorar la seguridad informática del instituto COTEL-TUNJA de acuerdo al modelo de defensa en profundidad promovido por Microsoft.	✓ Generar un informe que señale las distintas opciones de hardening que puede implementar el instituto de acuerdo al modelo de defensa en profundidad promovido por Microsoft. ✓ Indicar los costes de implementación de las medidas de hardening sugeridas

Fuente: El autor

7. HARDENING. ESTRATEGIAS Y DEFENSA EN PROFUNIDAD

El hardening de forma somera, es entiendo como el proceso de aseguramiento o endurecimiento de un sistema informático a través de bastiones de seguridad (capas u obstáculos), lo cual servirá para ralentizar y dificultar la actividad de un atacante en su tarea de vulnerar un sistema informático. Este concepto se aplica para el aseguramiento de sistemas que estén compuestos de hardware, software o una combinación de ambos, en ese caso el hardening aplica para la protección bien sea de un computador, una estación de trabajo, una red de computadores y su perímetro o en otros casos la protección de un programa o aplicativo informático. Así entonces, las medidas que se puedan implementar para un bastionado pueden variar de acuerdo al sistema y objetivo a proteger, como también los procesos o estrategias que se usen para ello.

7.1. ESTRATEGIAS DE HARDENING

La mayoría de estrategias apuntan al aseguramiento de un sistema en específico bien sea un sistema operativo o un computador, en esto lo más común que se implementa es la aplicación de un antivirus, el parcheo o actualizaciones constantes, así como el manejo de contraseñas seguras o el uso correcto de internet y dispositivos removibles. Por otro lado, si lo que se quiere es buscar vulnerabilidades en una red de computadores, se puede usar pentesting con el fin de hallar vulnerabilidades y luego corregirlas; también se puede hacer uso de un blue team, el cual consiste en un grupo que busca vulnerabilidades en un sistema informático a través de pruebas de ethical hacking.

Pero cuando se habla de un sistema informático en el cual se maneja una red de comunicaciones, flujo de información y varios usuarios, la tarea de protección ha de implicar una mixtura de opciones de seguridad las cuales han de transformarse en una estrategia integrada siendo una de ellas la de defensa en profundidad.

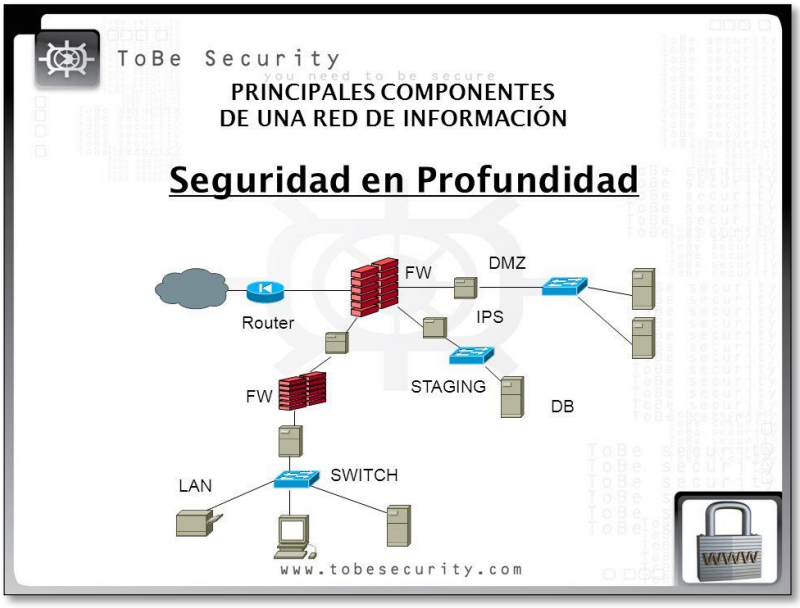
7.2. DEFENSA EN PROFUNDIDAD

Teniendo presente que el hardening implica realizar una seguridad a través de bastiones esto se enlaza directamente con el concepto de defensa en profundidad (Defense in Depth), este hace referencia a aplicar controles y medidas de seguridad

en diferentes capas cada una de las cuales representará el uso de una serie de tecnologías y procesos para hacer frente a amenazas informáticas.

A continuación, se puede ver un ejemplo de seguridad en profundidad en una red de computadores a través del uso de dos firewalls y una DMZ.

Figura 4. Seguridad en profundidad en una red de información



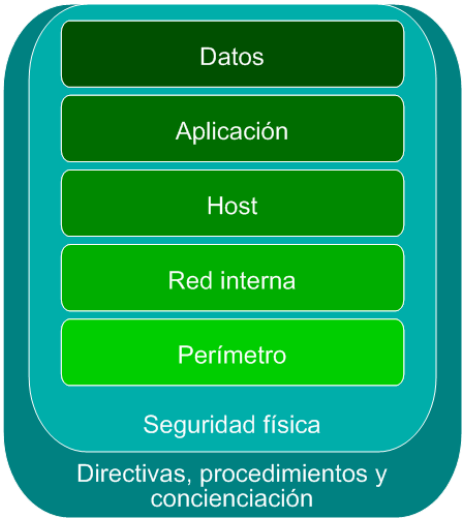
Fuente: http://slideplayer.es/slide/1055305/

El anterior grafico muestra una seguridad efectiva y robusta de acuerdo al concepto manejado, no obstante, no se tiene una forma de saber qué proceso se estableció para ello, debido a lo cual se requiere de un modelo de seguridad que indique la forma correcta en que se han de implementar las medidas de seguridad que se requieran siguiendo un proceso metodológico, razón por la cual se seguirá el modelo de defensa profunda que presenta Microsoft.

7.2.1. Modelo de defensa en profundidad Microsoft. El modelo de defensa en profundidad promovido por Microsoft está diseñado para implementar una serie de prácticas con el fin de asegurar sistemas redes de una organización en distintas capas, de tal suerte que cada capa ayuda a mitigar los ataques a medida que éstos avancen por cada una de las mismas, o visto de otra manera, para que un atacante llegue a un dato o información, debe poder vulnerar más de una medida de seguridad.

La documentación acerca de este modelo es muy variada incluso en la página principal de Microsoft, ya que no hay artículo que lo describa en específico sino que hay una colección amplia de ellos en donde se cita como referencia para temas de protección a través de productos de la misma compañía, es por ello que se tomará como referencia en primer lugar el artículo “Guía de defensa en profundidad antivirus”[47], en este se aprecia el grafico que ayuda a entender mejor el modelo.

Figura 5. Modelo de seguridad de defensa en profundidad



Fuente: https://technet.microsoft.com/es-es/library/cc162791.aspx

En segundo lugar, se cita el artículo “Windows Server 2008 en una Estrategia de defensa en profundidad de la compañía” de Jay Paloma en el cual se da una descripción somera del contenido de cada una de las capas de dicho modelo:

- “Datos. El blanco principal de un atacante, inclusive las bases de datos, la información de servicios del Directorio activo, documentos y más.
- Aplicación. El software que manipula los datos y que es el blanco principal del atacante.
- Host. Las computadoras que ejecutan las aplicaciones.
- Red interna. La red en la infraestructura de TI corporativa.
- Perímetro. La red que conecta la infraestructura de TI corporativa a otra red, como usuarios externos, socios o Internet.

[47] Richard Harrison. (Guía de defensa en profundidad antivirus). 2004. 2016, de Microsoft.com. Disponible en: https://technet.microsoft.com/es-es/library/cc162791.aspx

• Física. Los aspectos tangibles en informática: las computadoras-servidores, discos duros, conmutadores de red, fuentes y más.
• Conocimiento de políticas y procedimientos. Los principios generales que rigen la estrategia de seguridad de toda compañía. Sin esta capa, fallaría toda la estrategia"[48].

En ese sentido, La idea de este modelo es que todas las medidas de control interactúen entre sí formando una solución integrada desde la capa de directivas y políticas hasta la capa de datos, lo cual reduce las posibilidades de que exista un único punto de vulnerabilidad en un sistema informático.

7.2.2. Capas del modelo de defensa en profundidad Microsoft. A continuación, se explica cómo funciona la seguridad o procesos que se pueden aplicar en cada una de las capas del modelo de defensa profunda de Microsoft.

7.2.2.1. Datos. Consiste en la implementación de medidas que permitan manejar los datos de la organización de una forma efectiva y segura, esto se puede lograr con acciones como copias de seguridad (backups), prevención de pérdida de datos DLP (Data Loss Prevention), encriptación de información como por ejemplo EFS (Encrypting File System) o generación de lista de acceso ACL (access control list), entre otros.

7.2.2.2. Aplicación. esta capa es de vital importancia ya que implica el realizar prácticas para garantizar que las aplicaciones o programas sean seguros, para ello se pueden realizar auditorías constantemente. Con el fin de lograr seguridad en este nivel, se pueden adecuar soluciones en torno a políticas de contraseñas, fijación de controles y permisos de acceso de usuarios (usuarios estándar - administradores). En estaciones de trabajo Implicaría las opciones más comunes que se conocen de seguridad informática como el uso de antivirus, así como también la realización de auditorías tanto al sistema operativo como a los aplicativo es que este contenga.

[48] Jay Paloma. (2007). Windows Server 2008 en una Estrategia de defensa en profundidad de la compañía. 2016, de Microsoft.com. Disponible en: https://www.microsoft.com/latam/technet/articulos/articulos_seguridad/2007/diciembre/sv1207.mspx

7.2.2.3. Host: (Servidor) esta capa busca el aseguramiento de los servidores protegiendo los sistemas operativos de los mismos bien sea a través de actualizaciones, autentificación de las cuentas de usuario (con el fin de evitar intrusos locales o no autorizados), registros o logs de seguridad. En este punto se pueda hablar nuevamente de auditorías alrededor del tema de escaneo de vulnerabilidades lo cual se puede realizar por pentesting.

7.2.2.4. Red interna. En este caso la red interna de la organización, la cual puede ser local, inalámbrica o WAN (red de área extensa). En ese sentido implica realizar procesos que conlleven a la protección y el buen uso de esta red ya que de ella hacen uso inmediato los usuarios autorizados de la misma y por tanto la información que trasmitan en la misma es confidencial. Así pues, aplicarían medidas de seguridad como dividir la red interna en zonas de seguridad para establecer un perímetro alrededor de cada una de ellas, a este proceso se le conoce como subenteo o subnetting. También se pueden implementar sistemas de detección de intrusiones IDS, sistemas de prevención de intrusiones IPS, IPSec (Internet Protocol Security) y Firewalls.

7.2.2.5. Perímetro. Lo que se busca en esta capa es asegurar todo el perímetro de la red de comunicaciones de la organización, en este punto se pueden utilizar medidas como son las zonas desmilitarizadas, redes privadas virtuales (VPN), servidores de seguridad o Honeynets.

7.2.2.6. Seguridad física. El objetivo de esta capa es establecer todas aquellas medidas de seguridad sobre los activos físicos que tiene la organización, lo cual brindará protección contra intrusos que deseen sabotear o realizar daños físicos a nuestros sistemas, para ello se puede tener en cuenta medidas para protección contra hurto o ingreso físico no autorizado como sistemas biométricos, dispositivos de monitoreo, llaves físicas, tarjetas inteligentes, cámaras de seguridad (CCTV) alarmas, personal de vigilancia. De igual suerte, implica el hacer uso de equipos físicos auxiliares como reguladores de voltaje, UPS (Sistema de alimentación ininterrumpida), reguladores de temperatura para el caso de estaciones de trabajo que generen un alto nivel de calentamiento (por ejemplo, servidores en espacios cerrados o un DataCenter).

7.2.2.7. Políticas, Procedimientos y concientización. Esta capa como se observa en el modelo de Microsoft, es la que se encarga de proteger todo el sistema por lo tanto de ella harán parte los mismos usuarios de este de tal suerte que se conviertan en la primera barrera de defensa, para ello es necesario capacitarlos a través de la educación y concientización acerca de la normatividad, políticas de seguridad, así como procedimientos establecidos para hacer frente a lo que son desastres o la aparición de amenazas informáticas. Es de resaltar también como se debe documentar la seguridad y la preparación de planes de contingencia.

8. HARDENING EN WINDOWS

El hardening en Windows es una actividad obligatoria y más aún si toda una red de computadoras tiene presente versiones de este sistema operativo, esto debido a que como se comentó anteriormente, es uno de los sistemas operativos más atacados; en ese sentido la variedad de herramientas disponibles para bastionar estaciones de trabajo bajo este sistema es amplia y la implementación sencilla.

Las medidas que a continuación se enuncian aplican para toda versión comercial de Windows sea el caso de Windows 7, Windows 8, Windows 10, como también para las versiones server siendo estas Windows server 2008, 2012 o 2016 (no se mencionan las versiones anteriores XP o server 2003 por el fin de soporte de estas).

8.1. WINAUDIT

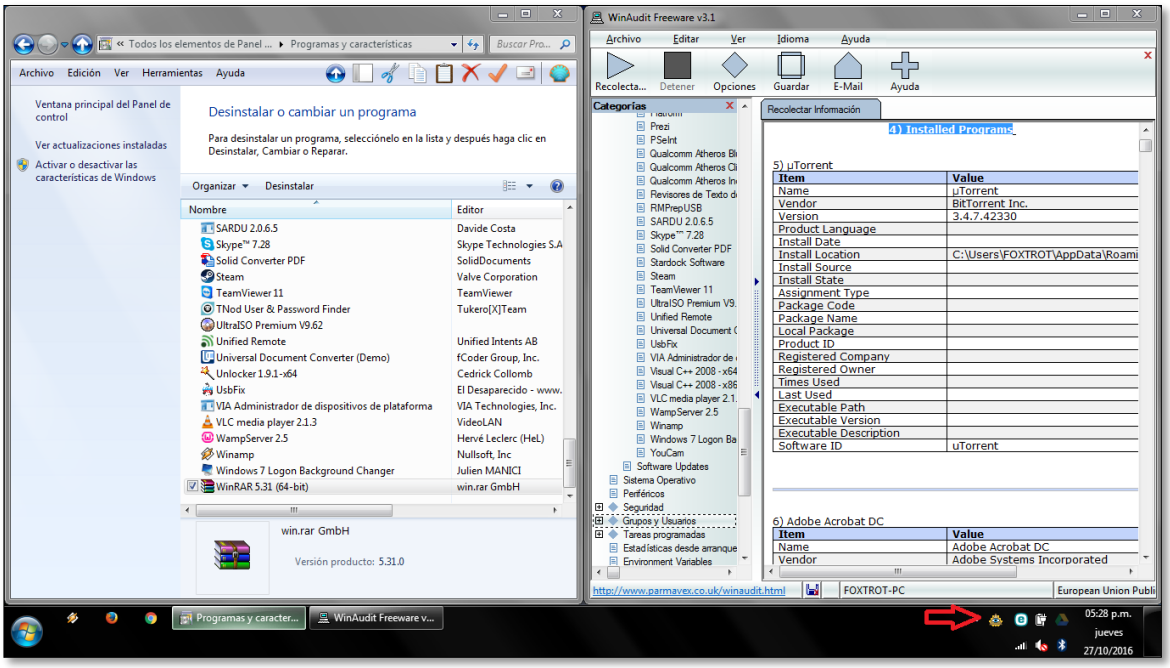
Es una aplicación de auditoria (tipo software TAAC) desarrollada por CodePlex cuya última versión estable es la v 3.1. Es de código abierto y de licencia gratuita. Con esta herramienta se puede auditar equipos de cómputo bajo Windows y ayuda a detallar la composición de software y hardware que esté presente, así como también indica las configuraciones de seguridad del sistema operativo y da una breve descripción de los programas que están presentes en este.

Una de las partes más importantes de este software es la pestaña seguridad, la cual brinda información acerca de los permisos que manejan los programa instalados detallando que hace cada uno. Otra pestaña importante es security settings en donde se da un reporte de las configuraciones de seguridad con los que operan las cuentas manejadas en Windows, así como programas. De igual suerte se puede obtener información del Windows firewall y los programas y puertos que tengan permisos de conexión.

Una de las desventajas de este software es que no registra programas que tengan la posibilidad de saltar este registro de instalación como el caso de keyloggers, un ejemplo de ellos es Ardamax, el cual permite habilitar o es habilitar este registro y por tanto puede o no aparecer en las opciones de desinstalación de programas y características de Windows, lo mismo sucede en el caso de WinAudit.

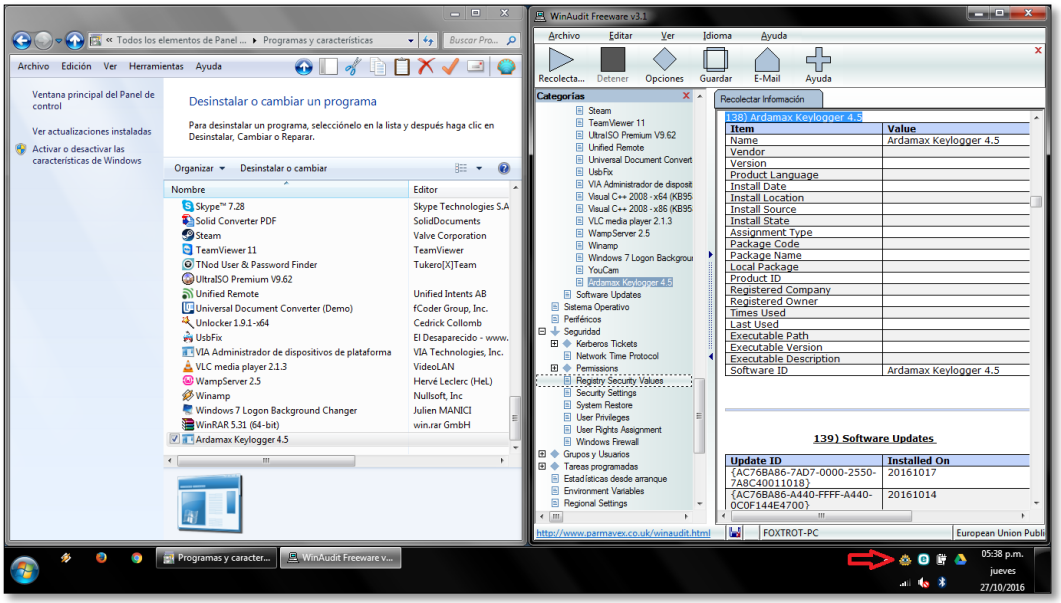
En las siguientes figuras se puede apreciar cómo está funcionando el programa Ardamax (keylogger) en Windows 7 sin registro de instalación y luego con registro habilitado en los entornos mencionados.

Figura 6. Ardamax sin registro de instalación



Fuente: El autor

Figura 7. Ardamax con registro habilitado



Fuente: El autor

Ventajas

- ✓ Permite hacer un inventario de los programas y configuraciones de la estación de trabajo bajo Windows

- ✓ A través de este programa se puede ver los permisos que tienen los programas respecto de su ejecución en sistema operativo

- ✓ Es posible ver las cuentas de usuario y sus distintos permisos, así como los que estén a establecidos a nivel general en la estación de trabajo

Desventajas

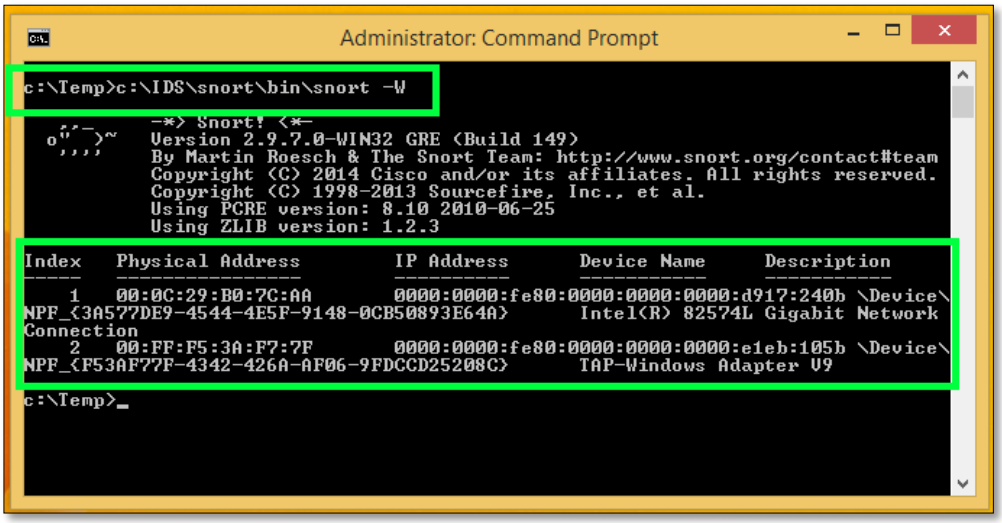
- ✦ No registra software que tenga la posibilidad de saltar el registro de instalación de programas en Windows

8.2. USO DE SNORT COMO IDS EN WINDOWS

Snort es un sniffer gratuito que sirve también como IDS en redes de tráfico moderado clasificándose como un NIDS (NetworkIDS o IDS basado en red) el cual detecta ataques en el segmento de una red. Se caracteriza por no implementar una interfaz gráfica, sino que se utiliza en modo consola en Windows (CMD); para su configuración y uso además del programa se requiere de una serie de librerías (libcap) así como también reglas (rules) que se pueden descargar del mismo sitio web del programa y las cuales poseen bases de datos de patrones de ataques o ataques conocidos.

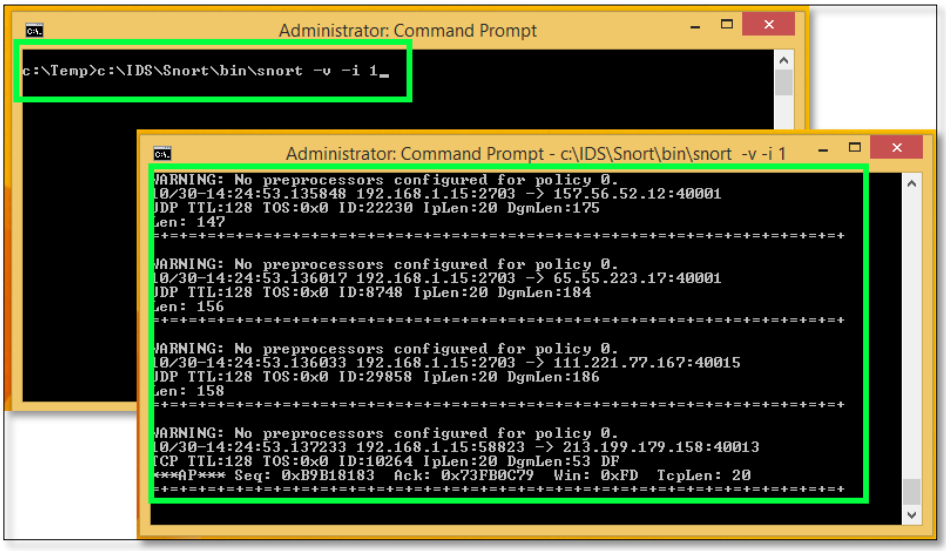
A continuación, se puede ver un ejemplo de su funcionamiento en el cual con el comando **C:\IDS\snort\bin\snort –W** se inicia un escaneo preliminar de dispositivos conectados, una vez que son detectados con el comando **c:\IDS\snort\bin\snort –v –i x** se comienza la escucha de los datos que están enviando o recibiendo esos dispositivos.

Figura 8. Escaneo preliminar con snort en Windows



Fuente: http://blog.muhammadattique.com/isnort-sensor-on-windows-with-remote-snort-using-winids/

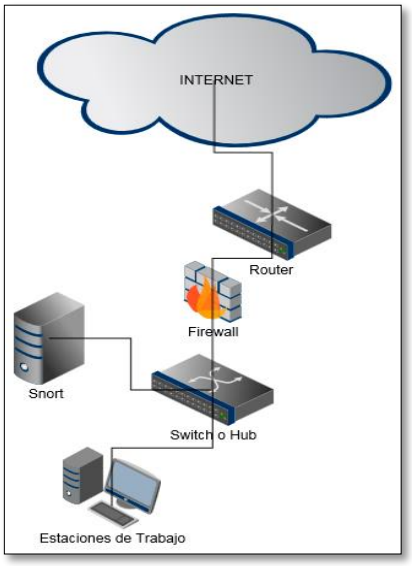
Figura 9. Inicio de escucha de tráfico en snort



Fuente: http://blog.muhammadattique.com/isnort-sensor-on-windows-with-remote-snort-using-winids/

La idea de usar un IDS es posicionarlo en un segmento de la red según el tráfico que se requiera vigilar bien sea de datos entrantes o salientes, dentro o fuera de un firewall, etc. En la siguiente figura se muestra el posicionamiento de una estación de trabajo con Snort la cual está capturando todo el tráfico interno de una red detrás del firewall de la misma.

Figura 10. Snort capturando tráfico interno



Fuente: https://www.joanesmarti.com/tu-propio-ids-con-snort-y-snorby-en-linux-debian-7/

Ventajas

- ✓ Permite la captura del tráfico generado al interior de una red, así como el que haya sido filtrado por el Firewall

Desventajas

- ✦ La falta de interfaz gráfica hace que su instalación y configuración no sea tan sencilla

- ✦ Se debe posicionar correctamente en una red, ya que un IDS soporta tráfico medio, por tanto, si se usa en el perímetro de una red que recibe muchas peticiones o entrada de datos puede saturarse dicho programa

8.3. SOFTWARE REBOOT RESTORE

Sirve para proteger el disco duro o las particiones de una estación de trabajo contra escrituras, en ese sentido lo que se busca es que la información, estructura y configuración del sistema operativo que está en un computador no sean modificados, permitiendo que los datos permanezcan inalterables a los cambios, a

este proceso también se le conoce comúnmente como congelar un equipo y al software como congelador. El funcionamiento de este software es bastante básico, una vez que es instalado se escoge que particiones del disco no quieren que sean modificadas, luego de ello cualquier dato guardado en la partición congelada será borrado luego de que el computador se reinicie, es decir, si por ejemplo se congeló el disco c y luego se instaló un programa en dicha partición, luego de que reinicie el pc el programa desaparecerá, así como los registros de instalación que haya hecho. Esto aplica para cualquier tipo de dato que se haya guardado, lo cual implica que luego de reiniciar se eliminara todo cambio que se haya hecho al sistema o todos los archivos que se hayan guardado de tal suerte que es una barrera excelente frente a indebidas manipulaciones de los usuarios, parches o actualizaciones que generen conflictos, o virus informáticos, este último por ser también un dato o archivo se borrará también.

En principio este tipo de programa está diseñado para organizaciones que manejen una planta de computadores extensa o de la que hagan uso varios usuarios, lo cual aplica en mayor medida que este sea usado para instituciones educativas, bibliotecas o cafés internet.

Un ejemplo de este tipo de software es Deep Freeze versión 8.23 (versión de prueba); en la siguiente figura se pude apreciar como en el proceso de instalación se puede escoger las particiones del disco a congelar (por defecto congela C: ya que ahí se guarda el sistema operativo en el caso de Windows).

Figura 11. Deep Freeze

Fuente: El autor

Ventajas

- ✓ Evita la modificación del sistema operativo en este caso Windows

- ✓ Es una barrera contra los virus informáticos ya que un virus al ser un dato informático cuando éste se guarda en un disco congelado es eliminado una vez que el sistema se restaure después de prenderse el computador.

Desventajas

- ✦ Alto consumo de memoria RAM: esto debido a que para impedir escrituras sobre el disco desvía parte este proceso a dicha memoria

- ✦ Para realizar cualquier cambio necesario sobre el sistema se debe descongelar o desactivar el programa, más una cuando se trate de programas que requieran reinicio para su correcto funcionamiento

- ✦ Si se tiene algún aplicativo que requiera actualizaciones, como por ejemplo antivirus, se requiere descongelar periódicamente para que el aplicativo este actualizado los más recientemente posible

Otras opciones además de software Reboot Restore son:

- Returnil
- Wondershare Time Freeze
- Windows SteadyState
- Comodo Time Machine
- Eax-Fix / Rollback
- HDGuard
- Drive Vaccine PC Restore Plus
- PowerShadow
- Shadow Defender

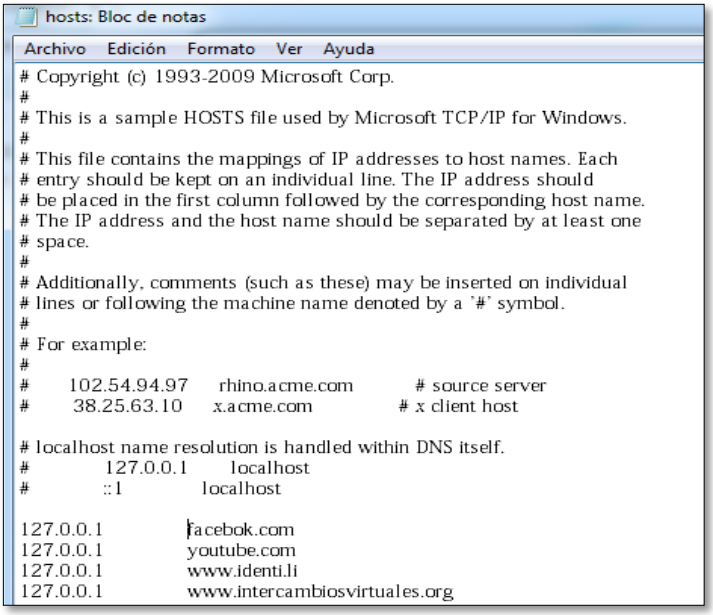
8.4. BLOQUEO DE SITIOS WEB A TRAVÉS DE ARCHIVO HOSTS EN WINDOWS

El archivo hosts de Windows es un archivo que maneja las conexiones de programas y sitios a internet bien sean salientes o entrantes. Este archivo puede ser utilizado para bloquear sitios de internet en la estación de trabajo sin necesidad de hacer uso del firewall de Windows o de un firewall físico (o en el caso de que falte alguno), esto ayuda a hacer más eficiente la labor de bloqueo de sitios y reduce costos en la labor de protección y seguridad informática.

Dicho archivo en Windows se encuentra en la siguiente ruta: C:\Windows\System32\drivers\etc

Una vez dentro de la ruta, el archivo hosts debe ser abierto con un bloc de notas tras lo cual aparecerá el contenido de este.

Figura 12. Archivo hosts



Fuente: El autor

Una vez dentro, todo sitio web que se desee bloquear se debe escribir en este bloc de notas precedido de la IP 127.0.0.1 y se guardan los cambios; como se observa en la figura anterior está bloqueado Facebook y Youtube además de otros sitios. Esta medida implica que se debe bloquear en este archivo tantos sitios como

considere conveniente lo que implica hacerlo manualmente, la desventaja de esto es que se debe hacer una lista amplia y creciente por la multitud de páginas que existen, en ese caso lo más recomendable es bloquear los sitios que más generen inconvenientes para la organización respecto de las costumbres nocivas de sus usuarios por ejemplo sitios de redes sociales, de streamming, de juegos, etc.

Este método lo implementan los firewalls físicos, el problema con ellos es que hay que pagar una licencia anual para tener en funcionamiento el firewall y que descargue una base de datos de sitios web a bloquear, lo cual representa un coste importante.

Ventajas

- ✓ Se puede bloquear sitios de forma rápida en una estación de trabajo sin entrar en costes directos

- ✓ Es una línea de defensa en caso de no disponer de un cortafuegos físico

Desventajas

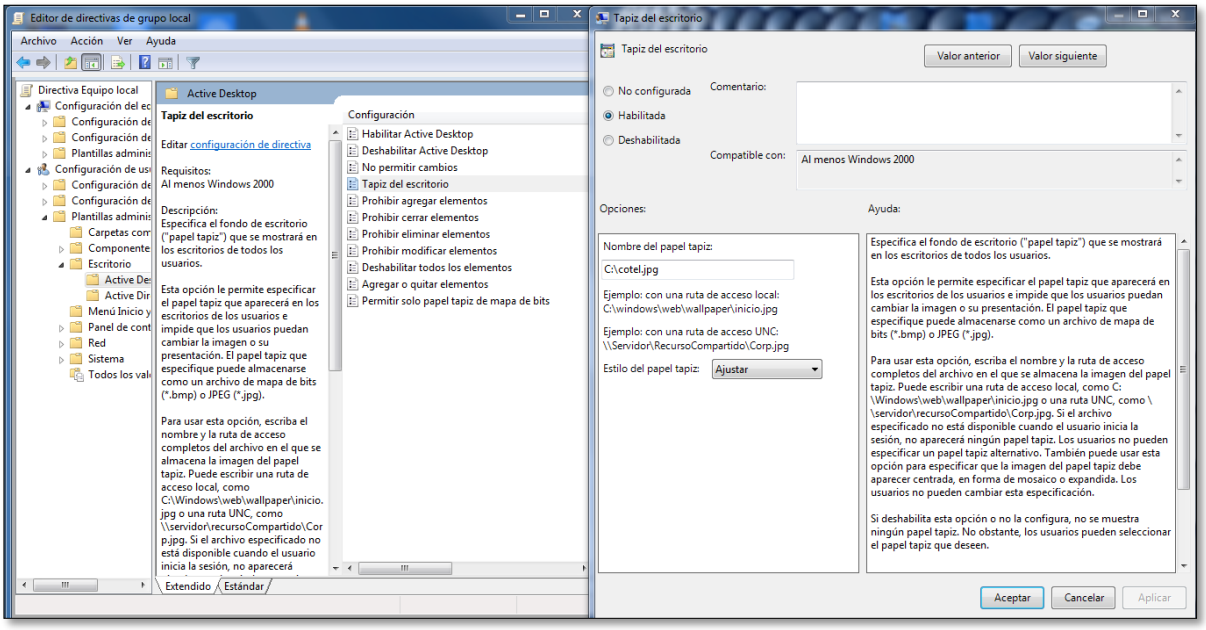
- ✦ Si se requiere ingresar a alguna página hay que modificar el archivo nuevamente

- ✦ Al no ser una solución final, la cantidad de sitios a bloquear puede ser muy amplia

8.5. USO Y APLICACIÓN DE GPO Y GPL EN WINDOWS Y WINDOWS SERVER

Para el caso de Windows comerciales (Windows 7,8 y 10) se habla de gpl (Local group policy o Directiva de Grupo Local) la cual se puede establecer a través del editor de directivas de grupo local o de forma rápida con el comando gpedit.msc en CMD (consola de comandos de Windows). En el siguiente ejemplo se puede apreciar como bloquear el protector de pantalla para impedir que sea modificado.

Figura 13. GPL en Windows 7 - bloqueo protector de pantalla



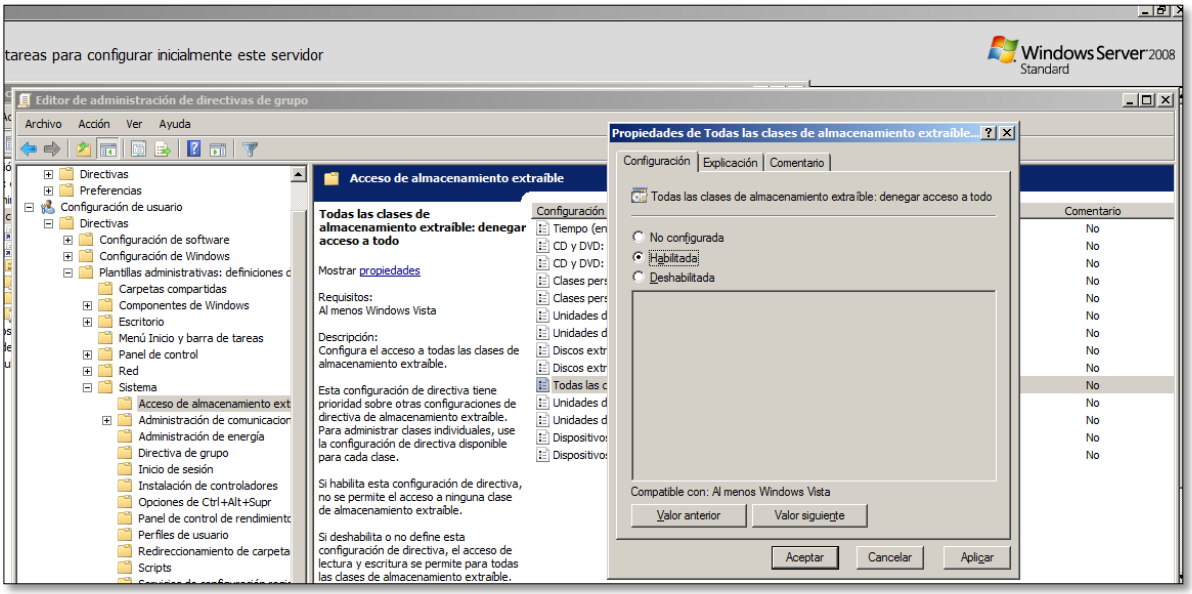
Fuente: El autor

En este caso este procedimiento se hizo sobre una cuenta de administrador, por tanto, para que surta efecto se requiere de la creación de una cuenta de usuario estándar con privilegios limitados de tal suerte que los usuarios que utilicen la estación de trabajo lo hagan siempre con esa cuenta y no con la de administrador, así no podrán revertir la configuración hecha.

Respecto de Windows server se implementa GPO (Group Policy Object u Objeto de directiva de grupo), este se configura en el editor de directivas de grupo y se pueden usar bien sea para grupos de trabajo o dominios de tal suerte que se puede aplicar medidas de seguridad y restricciones para todo un rango de usuarios o computadores desde un solo servidor sin necesidad de configurarlos uno por uno.

A manera de ejemplo se muestra la siguiente figura en donde se puede apreciar cómo se puede crear una GPO para el caso de bloquear el uso de dispositivos de almacenamiento USB en estaciones de trabajo que están siendo administradas por un servidor en Windows 2008.

Figura 14. GPO Windows server 2008 - bloqueo de unidades extraíbles



Fuente: El autor

Ventajas

- ✓ Se puede implementar medidas de seguridad en el mismo Windows y su interface sin hacer uso de otros programas

- ✓ En el caso de Windows server se pueden aplicar medidas de seguridad a un amplio rango de usuarios sin necesidad de configurarlos uno por uno lo cual ahorra tiempo y costes

Desventajas

- ✦ En el caso de Windows Server, al manejar GPO para grupos de trabajo o dominios, si se requiere instalar un programa hay que darle permisos a cada usuario que lo requiera, o, por otro lado, se pude implementar un GPO con un instalador, el problema de ello es que solo se puede usar archivos ejecutables con extensión .msi

9. HARDENING EN LINUX

Se puede decir que Linux llega a ser uno de los bastiones en hardening, esto en primer lugar debido que es un sistema que no permite la ejecución de programas sin autorización (no usa ejecutables .exe o registros), igualmente presenta una mejor configuración por defecto ya que el usuario tiene limitado sus privilegios o en el caso de ampliarlos debe configurarse para ello. Así pues, Linux se puede convertir es una de las barreras que se puede implementar en una defensa en profundidad, tal es el caso de su implantación como servidor lo cual es una actividad bastante común para proteger una red de computadores.

El hardening en esta plataforma parecería una situación no necesaria ya que en apariencia no es vulnerable, no obstante esto es un mito ya que es un sistema que si puede ser atacado, simplemente es uno que no es muy usado por la gente del común y por tanto el cibercrimen frente a este es reducido; los ataques que se pueden realizar a Linux en algunos casos son similares a los de Windows, como inyección de SQL o uso de ingeniería social, en otros casos incluso se pude hacer robo de la contraseña del superusuario (su) a través de scripts[49]. Otro ejemplo es el caso de Android el cual es el sistema operativo más atacado del momento incluso por encima de Windows y cuyo núcleo está basado en Linux.

A pesar de ello, Linux es susceptible de ser mejorado en cuanto a su seguridad, la ventaja de ello no solo reside en que es software libre, sino que, dependiendo de la distribución, las herramientas para ello pueden ser obtenidas de forma rápida y gratuita gracias a los repositorios a los que se pueda disponer, esto es un punto importante ya que no se pone en riesgo a las estaciones de trabajo frente a la búsqueda de cracks o activaciones que sean gratuitas ya que muchas de estas son trampas que llevan virus (sea el caso de troyanos y métodos phising).

9.1. HARDENING EN LINUX UBUNTU

Ubuntu por si solo implementa algunas medidas de seguridad por defecto sin embargo estas no garantizan su seguridad total, para solventar esto se puede modificar la configuración predeterminada o añadir software extra.

[49] OROVENGUA, J. (2015). Recuperar la contraseña de Root en Linux. Disponible en:http://www.linux-party.com/index.php/35-linux/8634-recuperar-la-contrasena-de-root-en-linux-o-hackear-tu-propio-sistema

La implementación de herramientas para esta distribución es amplia, así como los repositorios, no obstante, algunas han sido descontinuadas o sus proyectos solo funcionan en otras distribuciones Linux, tal es el caso de Bastille[50], la cual fue una herramienta de amplio uso en el hardening de Ubuntu pero que ahora está enfocada a distribuciones, Debian, Mandriva, o sistemas MAC.

En ese sentido, entras entre las medidas que se pueden aplicar para un bastionado en Ubuntu y herramientas para las mismas se tienen:

- “Instalar y configurar el Firewall – a través de ufw
- Asegurar la memoria compartida – a través de fstab
- SSH - Claves basadas en logueo, desactivar la conexión de la raíz (root) y cambiar puerto de logueo
- Apache SSL – Deshabilitar el soporte SSL v3
- Proteger el superusuario (su) limitando el acceso únicamente al grupo de administración
- Asegurar la red con ajustes en sysctl
- Desactivar la recursividad de apertura de DNS y de la versión Info - DNS Bind9
- Prevenir IP Spoofing (atasques de IP Spoofing)
- Bastionar PHP para mejorar la seguridad
- Restringir fuga de información de Apache
- Instalar y configurar la aplicación firewall de Apache – Se puede realizar a través de la instalación de la aplicación ModSecurity
- Protegerse frente ataques DDoS (denegación de servicio) con ModEvasive

[50] BASTILLE (2016). Disponible en: http://bastille-linux.sourceforge.net/

- Comprobar Registros y prohibir anfitriones sospechosos - implementando DenyHosts o Fail2Ban

- Usar sistemas IDS (Detección de Intrusión) – se puede realizar a través de PSAD

- Comprobar si hay rootkits - se puede realizar a través de Rkhunter y chkrootkit

- Escanear puertos abiertos - Nmap

- Analizar archivos de registro del sistema - LogWatch

- SELinux - Apparmor

- Auditar la seguridad del sistema Linux que manejemos – Tiger, Lynis y Tripwire"[51]

9.1.1. Lynis. Es una herramienta de auditoria usada en sistemas Linux, Unix and macOS así como otros basados en UNIX. Gracias a este software se puede determinar el estado de seguridad de un sistema a través de un proceso de exploración el cual se compone de las siguientes fases:

- "Determinación de sistema operativo

- Búsqueda de herramientas y utilidades disponibles

- búsqueda de actualizaciones de Lynis

- ejecución de pruebas de complementos habilitados

- ejecución de pruebas de seguridad por categoría

- generación de reporte de estado de análisis de seguridad"[52]

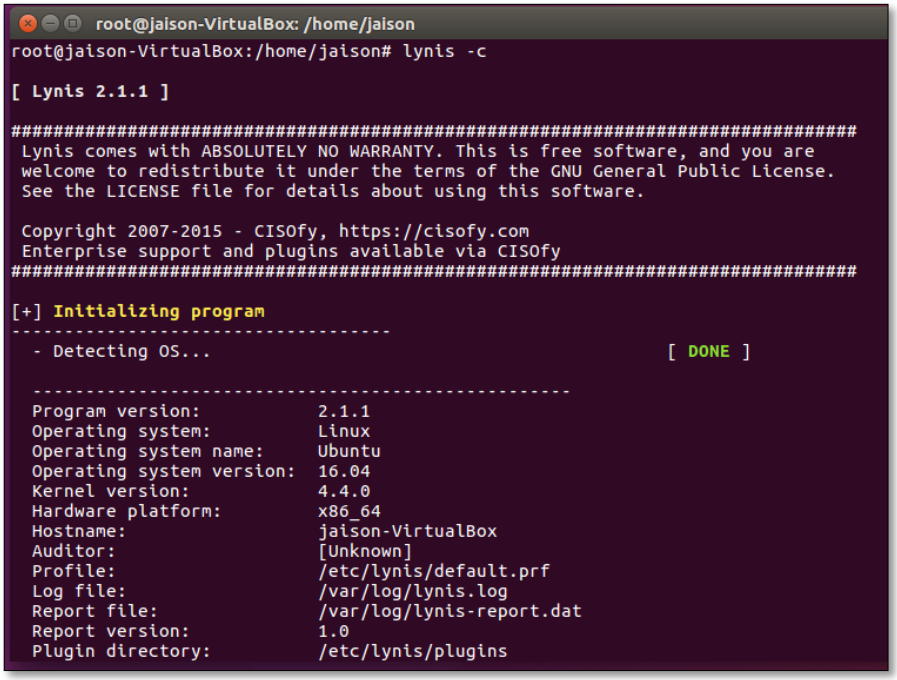
[51] Thefanclub (2016) How to secure an Ubuntu 16.04 LTS server - Part 1. 2016. Disponible en: https://www.thefanclub.co.za/how-to/how-secure-ubuntu-1604-lts-server-part-1-basics
[52] Cisofy. (2016). Lynis. 2016, de Cisofy . Disponible en: https://cisofy.com/lynis/

Esta herramienta fue creada por la compañía CISOfy de origen holandés, cuya labor es el desarrollo de soluciones de software para asegurar sistemas basados en UNIX (como Linux y macOS) con la finalidad de realizar auditorías de seguridad, endurecimiento de sistemas y pruebas de cumplimiento.

Esta aplicación está disponible en los repositorios de distintas distribuciones Linux como CentOS, Fedora, Debian, Redhat así como también para Ubuntu y su uso ayuda a profesionales de la seguridad informática a escanear el sistema y sus defensas de seguridad, con lo cual se logra determinar la información del mismo, el tipo de sistema operativo específico, paquetes instalados, configuración del sistema y de la red. De igual manera, esta aplicación verifica si existen errores de configuración y problemas de seguridad en el sistema.

Para descargarla en el caso de Ubuntu basta con instalarla a través de la Shell con el comando “apt-get install lynis”

Figura 15. Lynis en Ubuntu



Fuente: El autor

Entre las ventajas que se mencionan frente a este software están el que Puede ser usado en la mayoría de distribuciones Linux, así como en aquellos que estén basados en UNIX. En contraparte, una de las desventajas sería los reportes que genera los cuales están en inglés, esto no debería ser un problema para un ingeniero de sistemas, no obstante, el inconveniente resulta en que al ser entregado a una organización se debe pasar todo esto a español con su respectivo análisis técnico.

9.1.2. OpenVAS. (Open Vulnerability Assessment System), es un kit de herramientas de seguridad especializado en el escaneo y gestión de vulnerabilidades de seguridad en sistemas informáticos basado en la versión libre de Nessus (razón por la cual inicialmente se le nombraba como GNessU) , presenta un sistema abierto para la identificación de vulnerabilidades el cual puede realizar escaneos concurrentes hacia múltiples nodos de una red, así como temporizados. Vale señalar que, al ser software libre, la mayoría de los componentes están bajo la Licencia Pública General GNU (GNU GPL) siendo así también una de sus cualidades el ser multiplataforma tal suerte que se puede utilizar en otros sistemas como por ejemplo Kali Linux.

Para instalar OpenVAS en Ubuntu se debe instalar los repositorios de origen de este, ya que no se consiguen de los servidores de Ubuntu, igualmente es importante mencionar que se debe disponer de una herramienta que genere un servidor local para poder arrancar la interface del mismo.

Para la instalación de OpenVAS se debe digitar en consola:

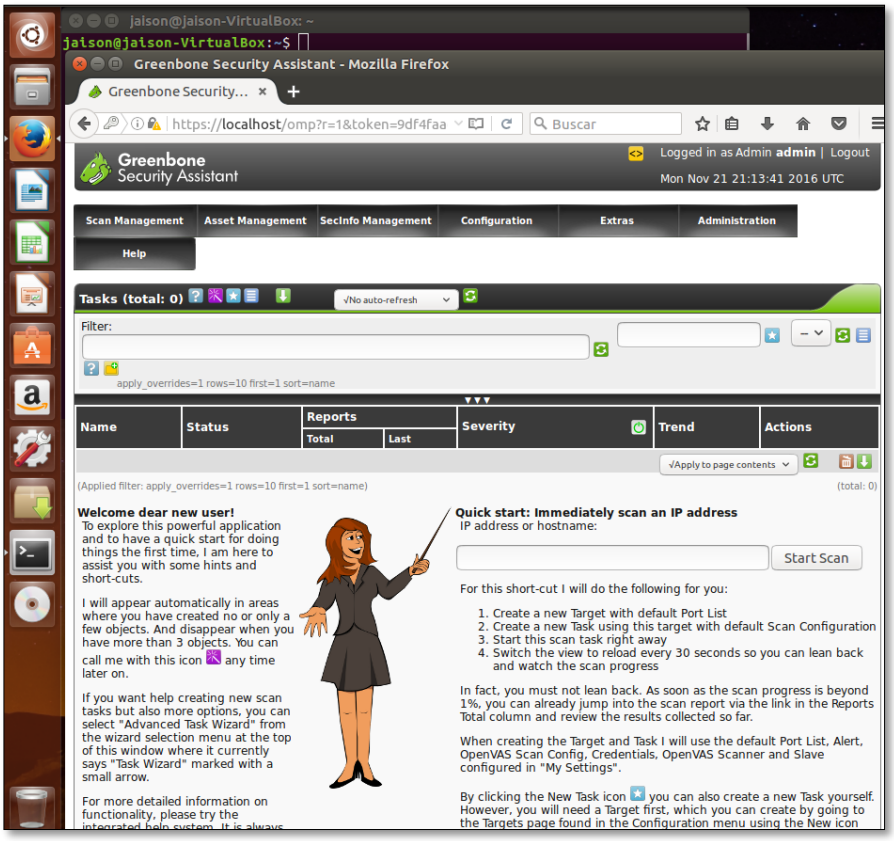
sudo add-apt-repository ppa:mrazavi/openvas

sudo apt-get update

sudo apt-get install openvas

Una vez que el software has instalado, para poder acceder a este se debe entrar a https://localhost/login/login.html, donde se pude tener acceso a la interfaz del programa

Figura 16. OpenVAS en Ubuntu



Fuente: El autor

Para el manejo de este software se dispone de un servidor web a modo de interfaz (Greenbone Security Assistant) para realizar las configuraciones necesarias en el mismo. Igualmente se acompaña con un base de datos de pruebas de vulnerabilidad de red conocidas como NVT (Network Vulnerability Tests) que se actualiza a diario y las cuales están conformadas por rutinas que verifican la presencia de un problema de seguridad específico que cumpla con una serie de patrones. La base de datos de NVT crece y actualiza semanalmente permitiendo a los equipos instalados con OpenVAS una sincronización con los servidores para actualizar las pruebas de vulnerabilidades.

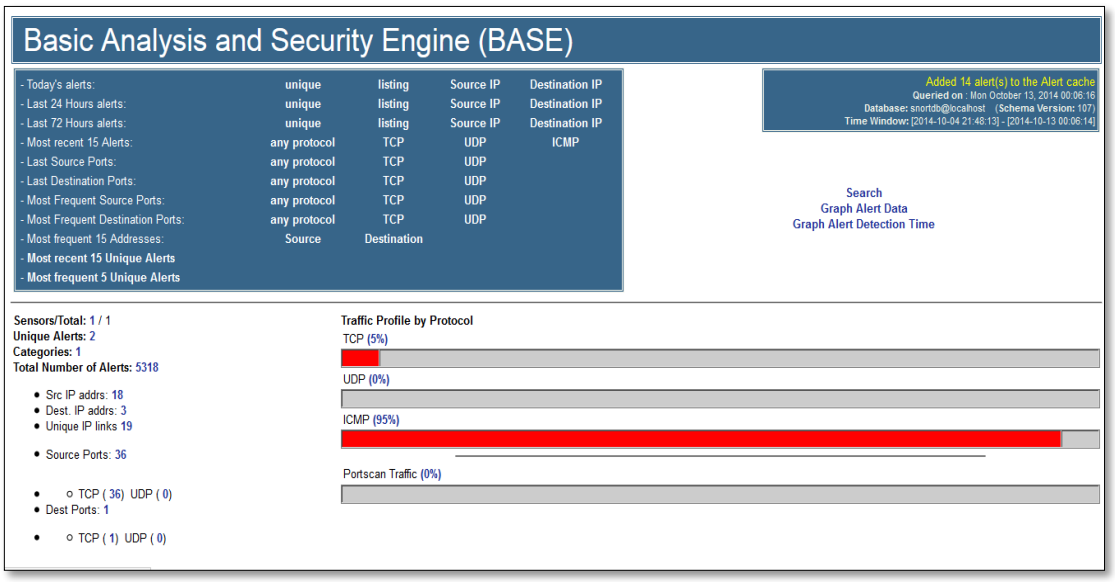
9.1.3. Snort. Es una de las herramientas más populares para labores además de ser un sniffer que permite ver en tiempo real todo el tráfico de paquetes que se mueven una red además que permite guardar los archivos de los para análisis offline sin necesidad de usar conectado a Internet), se caracteriza por ser NIDS (Network

Intrusion Detection System) aunque también puede realizar labores de NIPS (Network Intrusion Prevention System).

Este programa es de licencia abierta (GPL) y su instalación obviamente difiere de la que se hace en un entorno Windows ya que en este caso hay que dirigirse al repositorio para hacer la instalación del mismo con el Comando de instalación: apt-get install snort. No obstante, para la instalación efectiva de Snort**,** no basta sólo con instalar el programa, sino que también se requiere de software añadido como por ejemplo un servidor ssh, un servidor de datos (este caso se puede utilizar mysql o sqlite) y ethtool (para gestionar las configuraciones de tarjetas de red de forma más eficiente)[53].

Snort es un sistema susceptible de ser mejorado, por ejemplo, añadiéndole BASE (Basic Analysis and Security Engine)[54], siendo así que se pueda tener una consola de análisis Web que permita analizar los datos de Snort y almacenarlos en una base de datos de tal suerte que se puedan ver de forma sencilla las direcciones IP de los atacantes, fechas de acceso y demás datos.

Figura 17. SNORT con BASE en Ubuntu



Fuente: http://blog.muhammadattique.com/wp-content/uploads/2014/10/20-BASE-Dashboard.png

[53] UPADHYAY, R. (2016). How To Install Snort NIDS In Ubuntu 15.04. Disponible en: https://www.unixmen.com/install-snort-nids-ubuntu-15-04/

[54] ATTIQUE, M. (2015). Install and Configure Snort HIDS with Barnyard2, Base & MySQL on Ubuntu. Disponible en: http://blog.muhammadattique.com/install-configure-snort-hids-barnyard2-base-mysql-ubuntu/

Al igual que otros softwares Linux con licencia GPL, SNORT es multiplataforma pudiéndose implementar no solo en Windows y Linux sino también en aquellos basados en UNIX.

9.1.4. Inicio de sesión con verificación de dos pasos. En primer lugar, vale aclarar que la verificación de dos pasos (en inglés Two-Factor Authentication o **2FA)** consiste en que al acceder a un servicio informático que esté conectado a internet se requiera de un código especial y adicional la contraseña de usuario para poder ingresar, generalmente este código es numérico como el caso de un PIN (Personal Identification Number), el cual es enviado a un dispositivo móvil, bien sea a través de llamada telefónica o mensaje de texto (SMS), ejemplos de este método es el de acceso por seguridad a través de cuentas de Gmail, facebook o hotmail, entre otros.

En ese sentido frente a Ubuntu se puede utilizar este método de tal suerte que, al estar conectado a Internet, y usando Google Authenticator, se puede solicitar un código de acceso para entrar al login del sistema operativo y el cual es generado en un dispositivo móvil que también va estar conectado a Internet.

Para la implementación de este método de seguridad en Ubuntu se requiere de la instalación de Google Authenticator a través del comando **apt-get install libpam-google-authenticator**. Luego de ello es necesario arrancar el programa con **google-authenticator**, tras ello aparecerá una serie de preguntas respecto a la configuración del programa las cuales se aceptan (yes). Al final de esto el programa arroja dos códigos, un código QR para ser escaneado con un dispositivo móvil y un código en caracteres; estos dos códigos son los que se deben introducir en la aplicación móvil que se elija para generar el código de acceso.

A continuación, se observa una figura de google-authenticator en Ubuntu y la generación de los dos códigos anteriormente mencionados.

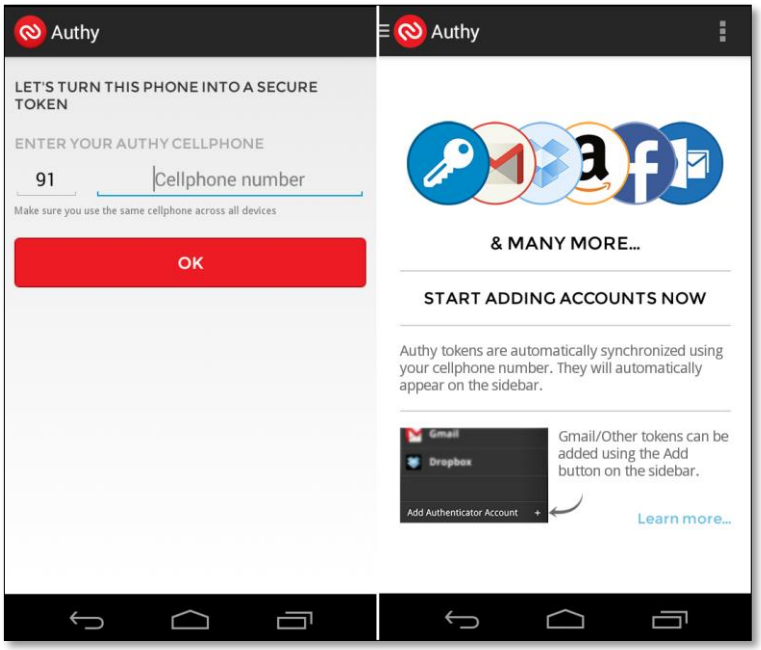
Figura 18. Google-authenticator en Ubuntu

Fuente: El autor

Luego de que ha sido instalado el programa se requiere una configuración en el archivo localizado en /etc/pam.d/lightdm, en el cual se debe añadir la línea **required pam_google_authenticator.so nullok** al final del mismo, esto para que Ubuntu requiera del código de acceso que ha sido generado en Internet para que permita entrar al sistema.

Respecto de la aplicación móvil que puede generar el código de acceso se pueden mencionar herramientas en Android como Authy, el cual reconoce los códigos QR y de caracteres generados por google-authenticator en Ubuntu y además permite generar el código de acceso; valga decir que este código de acceso va cambiando según lo configurado en el programa el dispositivo móvil de tal suerte que no puede ser el mismo cada vez que se solicita un nuevo código de acceso ya que irá cambiando como es lo usual en un sistema de verificación de los pasos.

Figura 19. Authy en Android



Fuente: http://www.elesconditefriki.com/wp-content/uploads/2016/06/Authy-1.png

Authy es una aplicación 2FA que no sólo permite autenticar códigos para google-authenticator, sino también para otros tipos de servicios en Internet ya sea servicio mensajería, redes sociales, nubes informáticas o aplicación comerciales.

Como se evidencia, esta medida de seguridad es bastante útil sobre todo para hacer frente a ataques de fuerza bruta, ya que así la contraseña de acceso al sistema no se verá comprometida, igualmente es importante mencionar que esta medida de seguridad es susceptible de ser mejorada implementando SSH (Secure Shell) , no obstante, la desventaja de este sistema es que se requiere de conexión a internet para acceder al sistema, entonces en caso de que no haya internet no se podrá loguear al sistema operativo.

10. ANÁLISIS PRELIMINAR DE VULNERABILIDADES DE COTEL-TUNJA

El Instituto COTEL-TUNJA, a pesar de ser una institución con varios años de experiencia en el sector académico, presenta una serie de vulnerabilidades y riesgos que pueden afectar de forma importante su desarrollo. En ese sentido se realizará un análisis de vulnerabilidades de acuerdo a cada una de las capas del modelo de defensa en profundidad promovido por Microsoft, esto con el fin de proponer opciones de hardening frente a los hallazgos reportados.

10.1. DATOS

- Falta de una base de datos: el instituto carece de una base de datos para manejar la información respecto de la planta estudiantil y docente, se ha detectado que únicamente se maneja registros de datos a través de hojas de Excel y que los reportes que se requieren a partir de las mismas no se dan de forma oportuna.

- No se realiza copias de seguridad: la información generada y administrada dentro de la institución, no tiene medidas de seguridad en el sentido en que no se aplican prevenciones para evitar su pérdida o sustracción por personal ajeno. En ese sentido no se realizan copias de seguridad ni se tiene programado un plan de realización de las mismas (ya sea diario, mensual o anual). En igual sentido es importante realizar cuando menos una copia de seguridad de esta información en algún servicio de la nube informática.

10.2. APLICACIÓN

- Falta de software de seguridad correcto: las medidas de seguridad implementadas en las estaciones de trabajo no son la idóneas, están instaladas con antivirus Security Essentials de Windows[55], el cual no es una buena opción de seguridad, no hay medidas extra de frente infecciones virales. Además, no se tiene definido planes de contingencia que impliquen software correctivo para hacer frente a infecciones virales o perdidas de información. A continuación, se muestra una figura de captura de pantalla de una estación de trabajo donde se evidencia la

[55] ROS, I. (2014). Windows Defender es el peor antivirus, según AV-Test. 2016, de muycomputer.com Disponible en: http://www.muycomputer.com/2015/03/26/windows-defender-peor-antivirus

instalación de Security Essentials, esto es igual en los demás computadores de la organización.

Figura 20. Security Essentials en estaciones de trabajo Cotel-Tunja

Fuente: El autor

➢ No se lleva un registro de las instalaciones de los sistemas operativos de las estaciones de trabajo, tampoco de los aplicativos que manejan y de la configuración que presentan. Esto indica que no se tiene una idea de cómo fueron instalados ni quien fue el encargado de realizar dicha instalación para poder descartar el uso de software malintencionado como keyloggers.

➢ Las estaciones de trabajo están configuradas con cuentas de administrador y por tanto son susceptibles de ser modificadas en cualquier momento. Además, que se les puede instalar cualquier programa por las mismas condiciones mencionadas.

10.3. HOST

➢ No existe ninguna medida de host: no hay un servidor que permita monitorizar la red o analizar el tráfico de comunicación en la red interna, ni tampoco que se sitúe como barrera de seguridad.

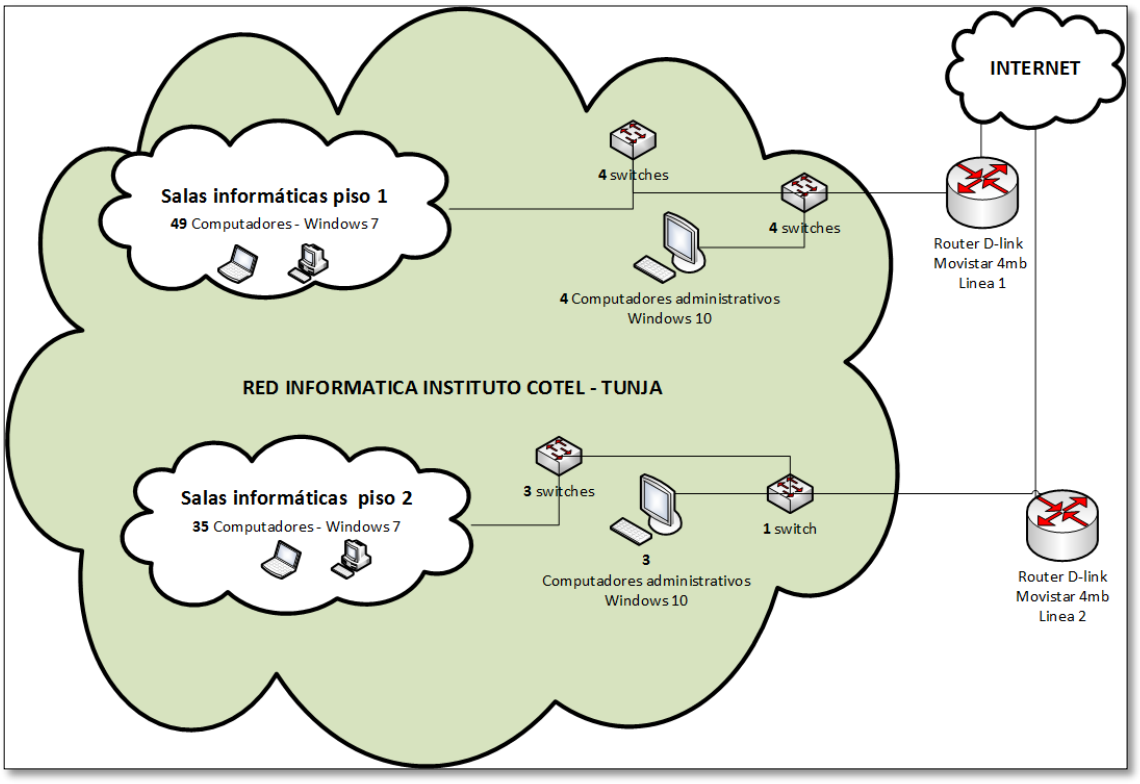
10.4. RED INTERNA

➢ Los usuarios de la red interna tienen acceso a cualquier contenido de internet, no hay ninguna medida que bloquee el acceso a páginas que causan alto tráfico y consumo de banda ancha, se evidencia que la mayor tasa de tráfico la genera YouTube y otros servicios de streamming, igualmente el acceso a redes sociales obstruye el buen desarrollo de las actividades laborales y académicas.

➢ El instituto presenta 2 líneas de internet de 4mb cada una, las cuales dan conectividad a todo el instituto, no obstante, todo el tráfico y consumo de ancho de banda lo consumen los estudiantes o las aulas informáticas que están conectadas, esto hace que las labores administrativas sean entorpecidas cuando hay alto consumo de internet.

Esto se evidencia en razón a que no hay una buena segmentación de la red interna tal como lo indica la siguiente figura en donde se representa en un diagrama la situación de la red.

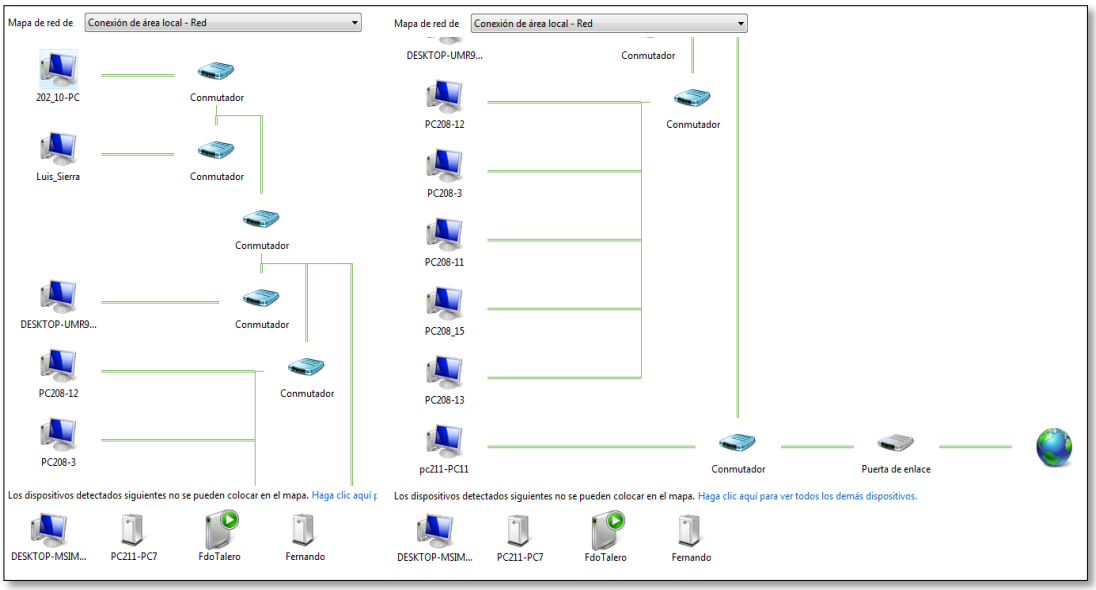
Figura 21. Diagrama red interna COTEL - Tunja



Fuente: El autor

➢ Existe una serie de grupos de trabajo de algunas salas informáticas que tienen compartición de archivos en la misma red del instituto, no obstante, estos grupos no están bien configurados y algunos entran en conflicto con otros o por el contrario tienen acceso a estaciones de trabajo no autorizadas desde la misma red.

Figura 22. Mapa de red de COTEL-TUNJA en Windows

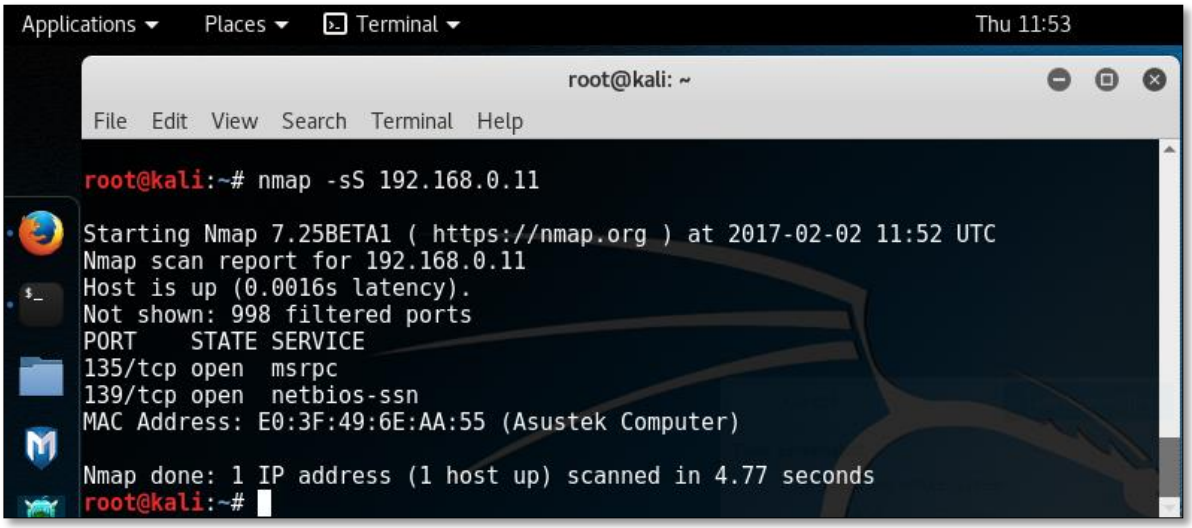


Fuente: El autor

10.4.1. Análisis de puertos abiertos con Nmap. Para verificar puertos abiertos se usó Nmap en Kali Linux 2016.2[56]. Se escogieron 3 computadores del instituto para dicha prueba como se muestran en las siguientes figuras.

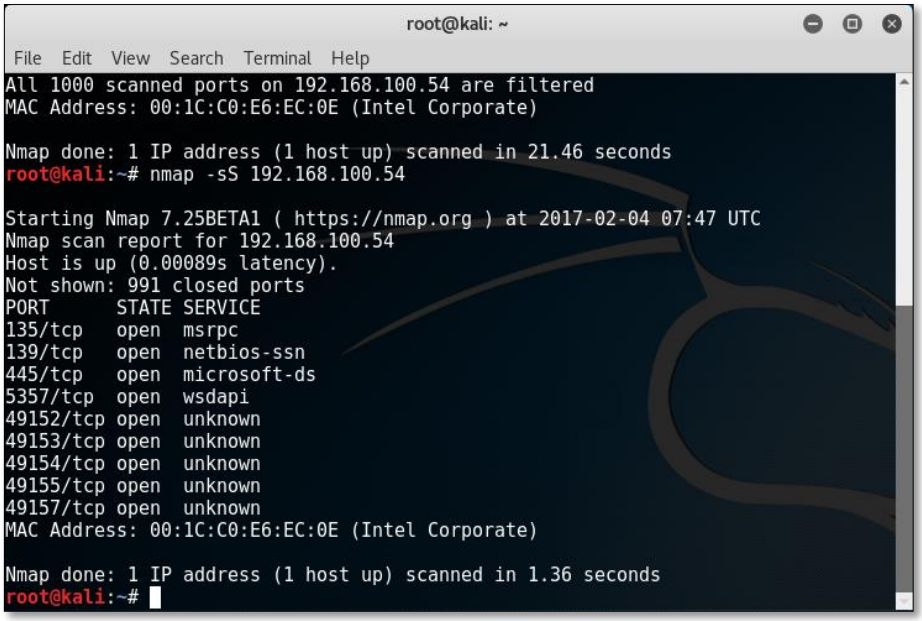
[56] Kali(2016). Kali Linux 64 bit. Disponible en: https://www.kali.org/downloads/

Figura 23. Escaneo con Nmap computador 1



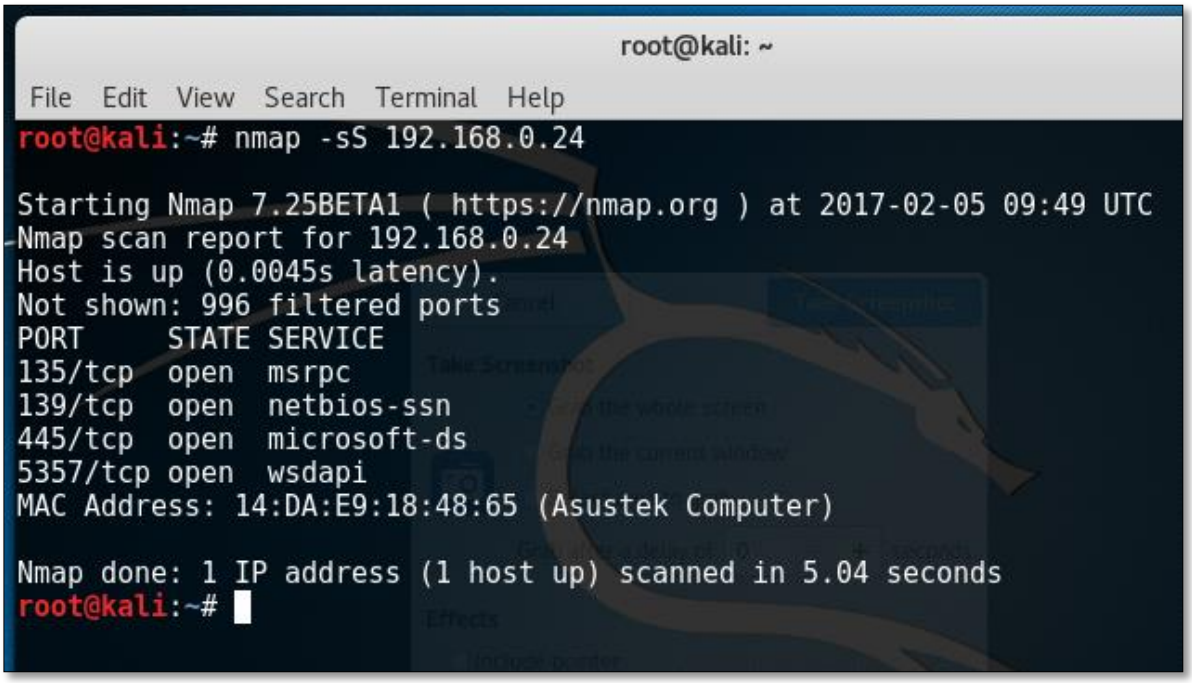
Fuente: El autor

Figura 24. Escaneo con Nmap computador 2



Fuente: El autor

Figura 25. Escaneo con Nmap computador 3



Fuente: El autor

Respecto del análisis realizado se pudo establecer que los puertos abiertos del computador 135 y 139 estaban abiertos debido a que carecía de antivirus, el computador 2 tenía el firewall de Windows desactivado razón por la que tiene 9 puertos abiertos y el computador 3 a pesar de tener instalado antivirus (security essentials) tiene 4 puertos abiertos.

10.5. FÍSICA

➢ Mantenimiento físico: la planta de computadores requiere de un mantenimiento físico para mejorar su funcionamiento o prevenir desastres. De igual suerte que es necesario realizarlo por cuestiones de salubridad y de acuerdo a un cronograma.

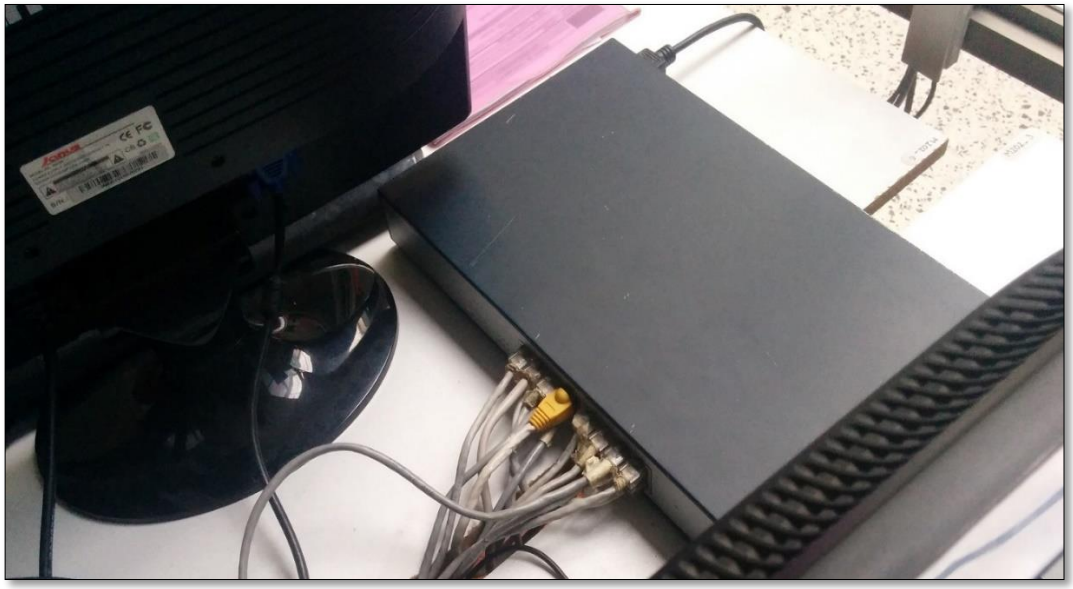
➢ Falta de cableado estructurado: no sea implementado de forma profunda una normatividad para estructurar el cableado de red (en este caso en UTP), algunos de los cables deben ser ponchados nuevamente.

10.5.1. Evidencia fotográfica cableado de red

Figura 26. Cableado de red COTEL-TUNJA 1

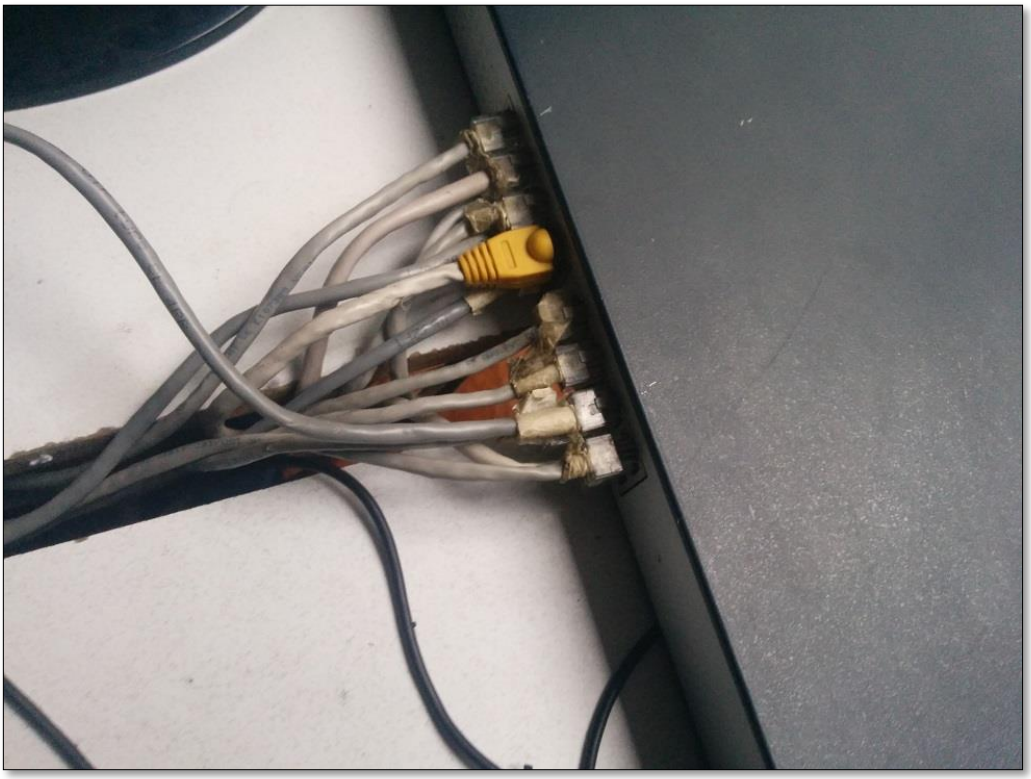
Fuente: El autor

Figura 27. Cableado de red COTEL-TUNJA 2



Fuente: El autor

Figura 28. Cableado de red COTEL-TUNJA 3



Fuente: El autor

10.6. PERÍMETRO

➢ El instituto presenta 2 WLAN (señales Wi-Fi), las cuales están configuradas con encriptación WPE, la cual puede ser vulnerada fácilmente, para realizar el análisis de ello y detectar el tipo de red que implementa las WLAN de cotel, en vez de utilizar un scanner en alguna distribución Linux (Kali por ejemplo) y tener que digitar comandos y configuración lo cual consume tiempo; se decidió utilizar un método más rápido que fue instalar la aplicación Wi-Fi Analyzer (open-source) [57] en un smartphone Android, dicha aplicación muestra las redes que están al alcance del dispositivo móvil y señala aspectos importantes como el tipo de encriptación, la intensidad de la señal, el tipo de dispositivo que emite la señal así como la dirección física de este. Con esos datos obtenidos de forma rápida se puede empezar un ataque para buscar la clave de acceso a una red inalámbrica. En la siguiente figura se aprecia el escaneo que nos arroja el programa en donde se evidencia las redes

[57] Wi-Fi Analyzer (2016). Disponible en: https://play.google.com/store/apps/details?id=com.vrem.wifianalyzer&hl=es-419

de COTEL-TUNJA y sus configuraciones, también se aprecia redes de otras organizaciones cercanas.

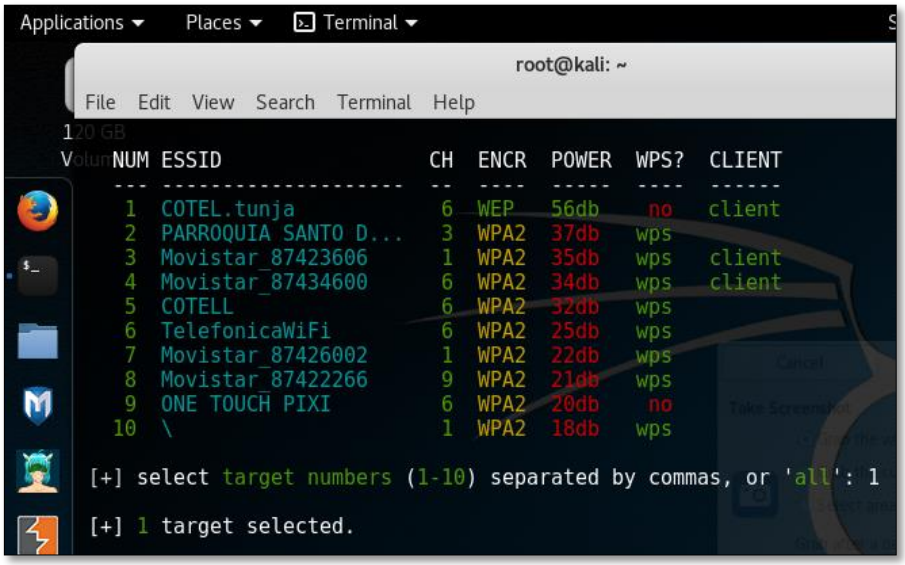
Figura 29. Análisis de redes Wi-Fi de COTEL a través de Wi-Fi Analyzer

Fuente: El autor

10.6.1. Análisis de vulnerabilidad red Wi-Fi (wlan) de Cotel con Kali Linux. Teniendo presente el estándar WPE que tienen configurado ambas redes del instituto, se procederá a hacer un ataque para obtener la contraseña de acceso de la red COTEL.tunja, esto con el fin de evidenciar la vulnerabilidad de la misma con fines de hacking ético.

Para la realización del ataque se utilizó Kali Linux, en ese sentido entrando al Shell se digita Wifite, esta utilidad permite realizar un ataque en búsqueda de contraseñas de redes wifi, implementando comandos conocidos como airdump-ng, aireplay-ng, entre otros de forma automatizada, así como también busca vulnerabilidades en WPS. Al arrancar Wifite lo primero que hace es buscar las redes cercanas y allí se escoge la que se quiere escanear (COTEL.tunja) como se aprecia en la siguiente figura.

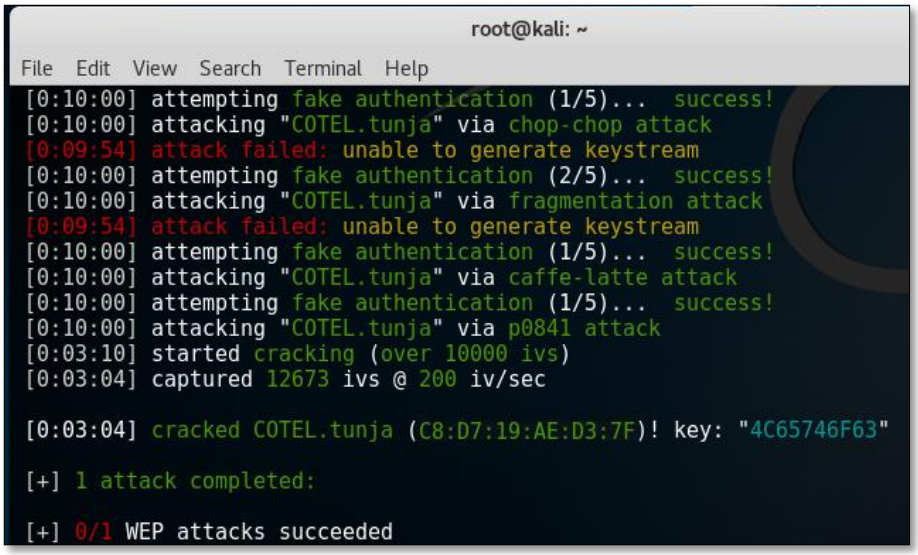
Figura 30. Escaneo red Wi-Fi COTEL.tunja con Kali Linux 2016.2



Fuente: autor

Una vez escogida la red empezará una serie de ataques para buscar la contraseña en la red WI-FI, esto lo hará de acuerdo al estándar de encriptación de la red, si tiene WPS activado o si hay algún cliente conectado, para ello busca que haya al menos un dispositivo conectado a dicha red y trata de desconectarlo de tal suerte que puede asumir su dirección MAC y así puede empezar a entrar al emisor de la señal WI-FI (Router) para iniciar la búsqueda de la contraseña. Esto se evidencia en la siguiente figura.

Figura 31. Ataque para búsqueda de contraseña de red Wi-Fi COTEL.tunja con Kali Linux 2016.2



Fuente: autor

Una vez que el proceso ha culminado, se puede apreciar como la contraseña de la red ha sido finalmente descubierta en el apartado de “key”. Esto sin duda alguna muestra la debilidad del estándar WPE en las redes del instituto ya que dicho proceso no tomó más de 10 minutos para arrojar el resultado del ataque.

Para verificar en nivel de seguridad de la contraseña descubierta se utiliza el sitio “How Secure Is My Password?[58]”, como nos muestra la siguiente figura 32, el sitio nos indica que la contraseña tiene un nivel bajo ya que puede ser descubierta en 1 día; el sitio hace este cálculo teniendo en cuenta la estructura de la contraseña, los computadores actuales y las formas de ataques informáticos modernos, no obstante y como se evidenció en la prueba de vulnerabilidad, el tiempo para descubrirla fue mucho menor.

Figura 32. Verificación de seguridad de contraseña en How Secure Is My Password

Fuente: autor

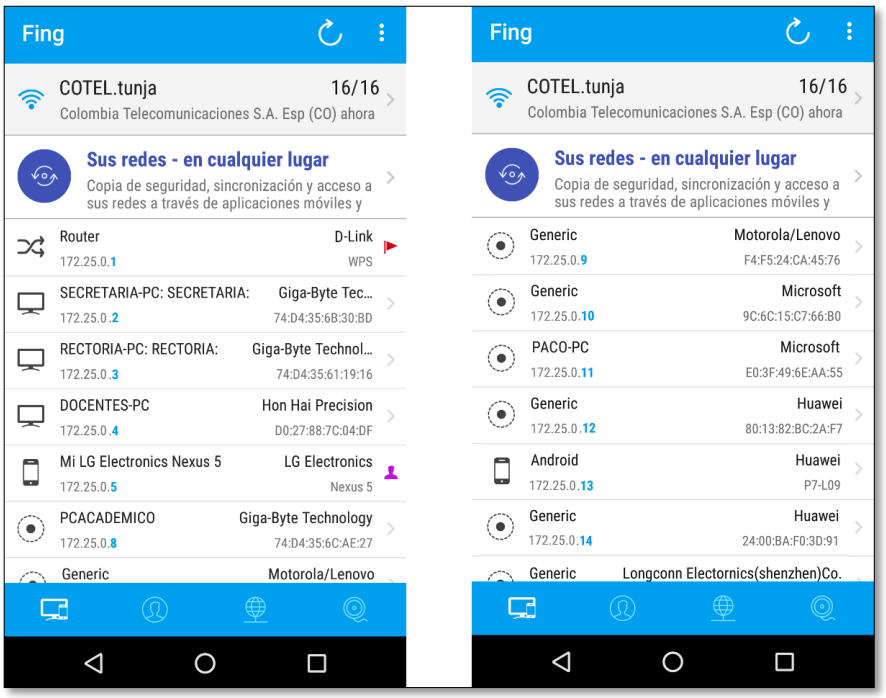
➢ A pesar de cambiarse la clave de las señales Wi-Fi, estas llegan a manos de terceros, sean estudiantes o personas ajenas a la institución, razón por la cual las directivas desean que el acceso de dichas redes WLAN se limite a una sola red y que sea permitido solo a determinadas personas a través de algún método más estricto o de lo contrario plantean cancelar las redes Wi-Fi.

10.6.2. Comprobación de usuarios ajenos conectados a red Wi-Fi (wlan) de COTEL. Para verificar qué otros usuarios ajenos han accedido a la red por fuera de

[58] How Secure Is My Password (2016). Disponible en: https://howsecureismypassword.net/

los administrativos se utiliza la aplicación para Android Fing[59], esta aplicación es un scanner de red que da información detallada acerca de usuarios y equipos conectados a una Wlan. En ese sentido se verifica que debido a que se propagó la contraseña de la Wi-Fi del instituto hay bastantes dispositivos ajenos conectados a la misma como lo evidencia la siguiente figura.

Figura 33. Comprobación usuarios conectados a red Wi-Fi COTEL.tunja con Fing



Fuente: el autor

➢ No hay ninguna medida de protección en el perímetro de la red del instituto frente a ataques externos, sea el caso de DMZ, firewall, entre otros.

10.7. DIRECTIVAS, PROCEDIMIENTOS Y CONCIENCIACIÓN

➢ Administrador de sistemas: se requiere un profesional en Ingenieria de Sistemas, cuya función sea la de mantener al día los sistemas computacionales y la red informática del instituto en torno al mantenimiento físico y lógico de los mismos, este profesional se encargará de diseñar e implementar estrategias y

[59] Fing (2016). Disponible en: https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=es_419

planes de seguridad para el manejo adecuado de los recursos tecnológicas del instituto de tal manera que mejore el rendimiento y uso de dichos recursos

- Falta de capacitación del personal técnico en sistemas: el personal técnico de sistemas requiere de una capacitación más profunda para hacer frente a los problemas que se dan en la planta computacional aun cuando se usan practicantes de la misma institución.

- Falta de políticas de seguridad: no se ha establecido ninguna clase de políticas para limitar y restringir el uso de los equipos informáticos frente a los usuarios o para que ellos hagan uso adecuado de la planta computacional.

- No se lleva un registro de hojas de vida de los equipos informáticos en donde se indique el contenido de los mismos (sea en hardware o software), sus modificaciones, actualizaciones o que muestre las personas encargadas de los últimos mantenimientos de estos.

- Falta de planes de concientización: no hay planes de concientización que indiquen tanto al personal docente y académico, así como el administrativo, en donde se les señale acerca del buen uso de las TIC en el instituto, así como las políticas que se implementan y la importancia de acatarlas y respetarlas.

- Falta de planes de contingencia: se requieren de planes de la generación de planes de contingencia en caso de desastres que afectan a la planta informática de instituto y que indiquen los procesos para salvaguardar los equipos y la información en caso de siniestros.

11. PROPUESTA OPCIONES Y RECOMENDACIONES DE HARDENING PARA COTEL-TUNJA

De acuerdo al análisis preliminar de vulnerabilidades y teniendo en cuentas las distintas opciones de hardening en Windows y Linux, se proponen las siguientes herramientas y medidas a implementar para los problemas de seguridad en el instituto COTEL-TUNJA.

11.1. DATOS

- Se requiere hacer uso de alternativas para manejo de información importante, el uso de aplicaciones de tipo web con arquitectura cliente-servidor, facilitan su uso y despliegue porque no requieren de instalación y mantienen la información centralizada y respaldada, en ese sentido se debe realizar el traslado o migración de la información contenida en las hojas de cálculo a un sistema de gestión de bases de datos como MySQL el cual se puede implementar en una aplicación web o plataforma web, en este caso se puede contratar el servicio de bases de datos con el hosting que aloja la el sitio web del instituto.

- Implementar una política y procedimiento de recuperación de desastres, donde se establezcan los lineamientos para la realización de copias de seguridad, la frecuencia y la identificación de información sensible. Tenido en cuenta aspectos como:

  • "Riesgos a los que se enfrenta la integridad y conservación de la información.
  • Importancia de la información.
  • Tipos de backup.
  • Dispositivos y tecnologías de almacenamiento.
  • Seguridad de las copias realizadas.
  • Acceso a la información guardada"[60]

Los backups de datos pueden abarcar desde archivos, sistemas operativos o instaladores de programas; en ese sentido los dispositivos de almacenamiento primarios han de ser unidades externas (discos duros externos), así también se recomienda el de programas para realizar clonado de discos, esto en razón a que

[60] Hernández, I. (2005). Métodos y Políticas de Respaldo (backup) en Planes de Contingencia 2016. Universidad Politécnica de Madrid. Disponible en: http://www.criptored.upm.es/guiateoria/gt_m001l.htm

la mayoría de motherboards son similares en los equipos y con copias de clonado se restauran estaciones de trabajo de forma más efectiva, este proceso se puede realizar con software gratuito como Clonezilla[61].

➢ El uso de servicios en nube informática garantiza la seguridad y fácil compartición, en este caso se sugiere no subir información sensible ya que los servicios en la nube pueden ser atacados bien sea por robo de identidad, phishing, keyloggers, entre otros. Así entonces pueden ser subidos archivos de publicad, presentaciones, publicaciones o información que sea de dominio público. Con esta medida se logra tener una copia de respaldo y se reduce la superficie de impacto de ataques virales ya que, si los archivos presentes en un pc son infectados, se pude recurrir a los de la nube para restaurarlos.

11.2. APLICACIÓN

➢ Se hace necesario implementar medidas de software antivirus de mayor efectividad que Security Essentials. En ese sentido se recomienda el uso de soluciones de seguridad Endpoint las cuales se caracterizan por permitir sincronización en la nube, control remoto de equipos, HIPS, control puede, entre otros. Siendo así, se sugiere la adquisición de Kaspersky Lab Endpoint Security [62] el cual es un producto de seguridad destinado a empresas (Endpoint Protection), se caracteriza por tener protección frente a ataques de día 0, detección de malware y bloqueos de falsas alarmas en sitios web, además que mejora la influencia del programa en la velocidad del computador en el uso diario, es decir no lo ralentiza tanto como otros antivirus en los análisis en tiempo real.

➢ Con el fin de evitar que los computadores sean modificados, se plantea La instalación de un servidor con Windows server e implementar ActiveDirectory con el fin de crear cuentas de usuario de acuerdo a los perfiles de usuarios dentro del instituto, con ello se procederá a crear GPO con el fin de bloquear modificaciones a las estaciones de trabajo impidiendo acciones tales como cambiar wallpapers, impedir inserción de dispositivos usb, restringir acceso a directorios, archivos o programas, entre otros.

[61] CLONEZILLA (2016). Disponible en: http://clonezilla.org/downloads.php
[62] AV-TEST. Ranking de antivirus empresariales 2016 https://www.av-test.org/es/antivirus/empresas-windows-client/windows-10/

- Realizar una auditoria con Winaudit para conocer la configuración de seguridad y los programas presentes en las estaciones de trabajo tras lo cual se podrá establecer un inventario de los programas usados y las configuraciones de seguridad a mejorar.

- Las estaciones de trabajo manejan Windows 7, se propone reinstalar el sistema operativo completamente en todos los computadores y verificar que dichas estaciones de trabajo presentan sus programas de forma correcta y no haya rastro de ningún software no autorizado; igualmente se verificará que presenten cuentas de usuario limitadas y que tengan restringido el acceso a sitios web. Estas acciones garantizaran que no se permita modificar su configuración y segundo, se verificará que no se haya instalado ninguna aplicación de tipo nociva sea el caso de keyloggers u otros.

11.3. HOST

Se propone Usar un servidor Ubuntu con versión 16.04 desktop, el cual se usará para monitorizar la red usando SNORT junto con BASE, para analizar de forma más sencilla el tráfico de red y de igual forma detectar intentos de intrusión. En este caso se usará con versión grafica para facilitar el trabajo de análisis además que no hará labores más allá de esta.

En el anexo A del presente trabajo, se puede observar una auditoria en Lynis a unos de los equipos de Cotel el cual será usado como servidor de monitoreo.

De Igual manera, para verificar que sólo acceda del administrador de sistemas al servidor se plantea el uso de un sistema de verificación de dos pasos con google-authenticator.

11.4. RED INTERNA

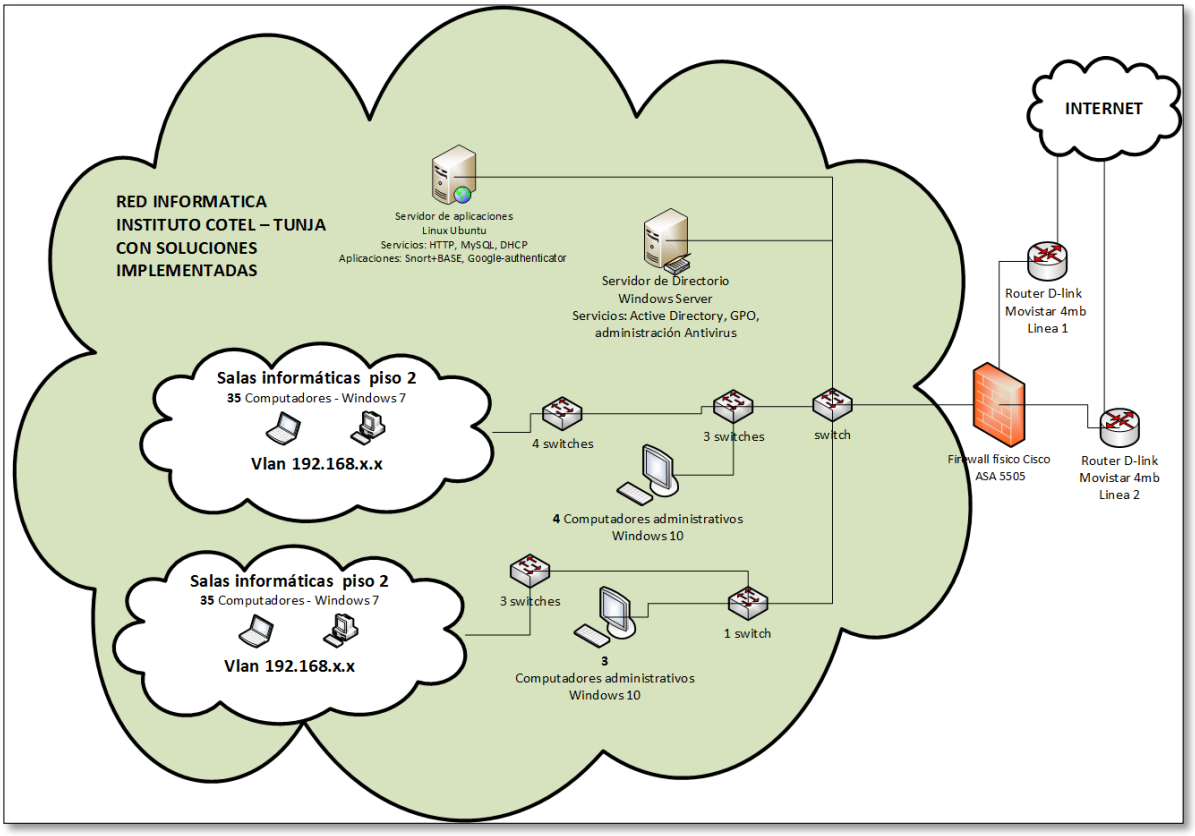
- Se propone realizar bloqueo de sitios web nocivos que más generan inconvenientes en la institución y que afectan las labores académicas y/o administrativas, como el caso de redes sociales, servicios de streaming, páginas de juegos, entre otros; en ese sentido se debe implementar un servidor Windows server el cual a través de políticas de grupo (GPO) bloqueará y filtrará el acceso a determinados sitios web; de igual manera el uso de listas de control de acceso

(ACL) ayudara a mejorar estas restricciones dando o limitando permisos de acuerdo a los tipos de usuario.

➢ Frente al manejo y distribución de internet, se recomienda segmentar la red de comunicantes haciendo uso de VLANs para restringir el tráfico entre las redes que se lleguen a crear. Esto con el fin de eliminar el colapso que sufrían las áreas administrativas por el alto consumo de ancho de banda de las aulas informáticas.

Con el fin de visualizar la implantación de tales medidas se presenta el siguiente diagrama que muestra cómo se daría el uso de las recomendaciones mencionadas junto con las demás contenidas en las propuestas de mejora.

Figura 34. Diagrama red interna COTEL – Tunja con soluciones



Fuente: El autor

➢ Frente a los puertos abiertos se recomienda verificar que el firewall este activado en los computadores e instalar un antivirus más robusto.

11.5. FÍSICA

➢ Mantenimiento físico: se propone el diseño de un plan de mantenimientos físico que sea periódico y que implique en mayor medida limpieza física de componentes. Esto con el fin de prolongar la vida útil de los componentes computacionales, así como garantizar medidas de higiene.

➢ Implementar Cableado estructurado: se hace necesario cambiar la categoría de cable UTP de 5e a 6 para mayor fiabilidad. Igualmente se recomienda el volver a realizar un mejor ponchado de los cables que presenten averías con conectores rj45 blindados categoría 6 aplicando la normatividad EIA/TIA 568A-568B. En igual sentido es importante efectuar un etiquetado de los puntos de red con el fin de identificar de forma más simple la ubicación de todos los cables de comunicaciones y puntos de red dentro del instituto, esto siguiendo los lineamientos de la normativa de rotulado TIA/EIA-606A[63]. Para la implementación del cableado estructurado a nivel del edificio se recomienda seguir la normatividad ANSI/TIA/EIA-568 (cableado horizontal, vertical y de usuario), ANSI/EIA/TIA 569 (limitaciones de cableado y niveles de interferencia) y ANSI/EIA/TIA−606 (métodos para la administración de los sistemas de telecomunicaciones)[64].

11.6. PERIMETRO

➢ Se propone la adquisición de un Firewall físico Cisco ASA 5505[65], esto en razón a que este dispositivo permitirá proteger la red interna frente ataques del exterior, además que su precio será económico y de fácil consecución en el mercado colombiano. Las características de este dispositivo van desde implementar antivirus propio el cual monitoriza desde los recursos de la red hasta el Gateway (puertas de enlace); evita ataques de spyware vigilando el tráfico por http, ftp o correo electrónico; presenta barreras anti-spam y anti-phising. Realiza monitorización en tiempo real frente al acceso web y transferencia de archivos. Igualmente permite realizar filtrado de URL, web e e-mail.

[63] Norma de cableado 606 (2008). Rotulado de cables y espacios. 2016. Disponible en: http://normasdecableado606.blogspot.com.co/2008/04/resumen-norma-606.html
[64] Universidad de Buenos Aires. Facultad de ingeniería. (2008) cableado estructurado (2016). Disponible en: http://materias.fi.uba.ar/6679/apuntes/CABLEADO_ESTRUC.pdf
[65] Cisco ASA 5505 (2016). Disponible en: http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733510.html

- Se debe Implementar el estándar de seguridad WPA2 en la red Wi-Fi que se establezca para la institución, esto se hace a nivel de la configuración respectiva del router D-link que la esté operando.

- SSID oculto: El SSID (Identificador de Conjunto de Servicios) es el nombre identificable de una red Wifi, por tanto, se sugiere configurarla de modo que se oculte su SSID y así la única forma de conectarse a esta sea a través de conexión manual en el caso de Windows[66].

- Igualmente se recomienda hacer uso de contraseñas más complejas para la seguridad de las redes wifi.

- Debido a que se requiere que solo a la red Wi-Fi puedan acceder únicamente los directivos del instituto, se recomienda dejar operativa sólo dicha red sobre la línea de internet del personal administrativo y docente; sobre la misma se debe efectuar un filtrado MAC de tal suerte que sólo admita aquellos dispositivos que ya han sido conocidos con anterioridad y que pertenezcan al Instituto o al personal autorizado, con ello aún si la contraseña de la señal Wi-Fi es compartida, no se dará acceso a Internet si no se encuentra en la lista blanca del filtrado MAC. Esto se realiza sobre la configuración de cada router, en este caso sobre el router D-link de la línea Internet del personal administrativo y docente que se lleguen a establecer.

11.7. DIRECTIVAS, PROCEDIMIENTOS Y CONCIENCIACIÓN

- Administrador de sistemas: se requiere de un profesional idóneo que mantenga al día los sistemas computacionales del instituto en torno al mantenimiento físico y lógico de los mismo, que proponga estrategias y ayude a implementar planes de seguridad y manejo adecuado de las herramientas tecnológicas del instituto. Ello en razón a que esa labor no puede está encomendada un técnico de sistemas el cual tiene menor experiencia y solo se encaja de los procesos de mantenimiento correctivo, pero no así de la seguridad informática.

- Capacitación y concientización: se hace necesario capacitar al personal administrativo, docente y académico en el uso correcto de los dispositivos computacionales que ofrece el Instituto reconociendo aquellas labores que pueden realizar en los mismos y aquellas que deben limitar, igualmente compete el

[66] Porras, A. ¿Es más Seguro Ocultar el SSID Wifi de mi red? (2016). Disponible en: http://www.soporteparapc.com/2014/08/ssid-wifi-oculto-es-seguro-o-no.html

capacitarlos en temas básicos sobre seguridad informática y buen uso de las TIC, así como también frente a las políticas que implemente el Instituto frente a ello.

- Establecimiento de políticas de seguridad informática: establecer medidas de acceso de acuerdo los perfiles de usuarios que se presentan y de acuerdo a las estaciones de trabajo, de tal suerte que puedan catalogar las tareas propias que se deben en los equipos de cómputo y la red de comunicaciones y aquellas que no.

- Implementar un registro de hojas de vida para que se pueda llevar un control de las modificaciones de los equipos informáticos y del software de los mismos y así tener un conocimiento exacto de las manipulaciones que se hacen sobre la planta computacional.

12. COSTOS DE IMPLEMENTACIÓN DE LAS OPCIONES DE HARDENING PARA EL INSTITUTO COTEL-TUNJA

Tabla 3. Medidas hardening propuesta-costos COTEL-TUNJA

CAPA DE DEFENSA EN PROFUNDIDAD	MEDIDA EN HARDENING	COSTO DE LA MEDIDA
Datos	Ampliación del plan de hosting web. Creación de base de datos y aplicativo web. Migración de datos a aplicación web *	$5'000.000
	Disco duro externo *	$200.000
	Subir información a google drive **	$0
Aplicación	Kaspersky Lab Endpoint Security (paquete de licencias por volumen)[67] *	$5'000.000
	Auditoria con WinAudit **	$0
	Reinstalación Windows 7 y programas en estaciones de trabajo **	$0
Host	Montaje servidor de monitoreo Ubuntu **	$0
	Montaje servidor Windows Server **	$0
Red interna	Configuración y redistribución de líneas de internet **	$0
	Segmentación de red **	$0
Física	Mantenimiento físico **	$0
	Cableado estructurado *	$2.000.000
Perímetro	Firewall físico Cisco ASA 5505 *	$2'300.000
	Implementación de WPA2 en red Wi-Fi **	$0
	Filtrado MAC **	$0
Directivas, Procedimientos y concienciación	Administrador de sistemas ***	$2.000.000
	Capacitación y concientización **	$0
	Establecimiento de políticas de seguridad informática **	$0
	Creación y registro de hojas de vida PCs**	$0
Total		$16'500.000

Fuente: El autor

* Se compra o se contrata con particulares

** Lo puede realizar el mismo administrador de sistemas con ayuda de técnicos practicantes razón por la cual el costo es $ 0

*** Implica que el ingeniero de sistemas sea contratado de planta o nómina

El coste total del proyecto para el instituto es de: $16'500.000 pesos m/cte

[67] Compra Kaspersky Lab Endpoint Security paquete de licencias (venta por cotización) Disponible en: https://latam.kaspersky.com/small-to-medium-business-security/how-to-buy

RESULTADOS

Los problemas informáticos que enfrenta el instituto COTEL-Tunja son problemas comunes en entornos educativos en donde se tiene que manejar un gran volumen de usuarios y la mayoría de ellos son inexpertos en el uso y buenas prácticas de las tecnologías de la información, así como en seguridad informática, por tanto, esta población se convierte en el principal foco de problemas informáticos al interior de una organización.

Tomando como referencia el análisis preliminar de vulnerabilidades y al manejo de la información los datos y registros de la comunidad estudiantil y educativa, se refleja el uso inadecuado de las herramientas informáticas en tanto que no se hace uso del concepto básico automatización de la información, lo cual implica que se utilicen bases de datos en vez del manejo de hojas de cálculo siendo así que además estas puedan ser protegidas a través de copias de respaldo bien sea en un aplicativo web o en una nube informática.

Igualmente es de reseñar como la red interna y el manejo de la banda ancha de Internet se encuentra colapsado en primer lugar por la permisividad frente al acceso de cualquier contenido a Internet desde cualquier estación de trabajo, y en segundo lugar debido a que no hay una segmentación o división de redes de computadores al interior de la institución.

Se evidencia como la falta de un administrador de sistemas de redes ha posibilitado la aparición de distintos problemas de seguridad en la institución, tanto físicas como en software, siendo así que las labores de mantenimiento del sistema informático y de redes de la institución se le han encargado únicamente a un técnico sistemas lo cual ha hecho que la parte de seguridad informática en general haya sido descuidada.

Un punto importante es el de la confidencialidad de los datos en cuanto a la exposición constante de las claves de acceso a las señales Wi-Fi, en ese sentido se evidencia que no hay un control estricto frente a la misma, razón por la cual es que es aún más necesaria la presencia de un administrador de sistemas para solventar los problemas de fuga de información.

El mayor problema se centra en la falta de políticas de seguridad, así como en la deficiencia de procedimientos y planes de concientización lo cual ha derivado en un

uso indiscriminado tanto de las estaciones de trabajo del Instituto como de un uso desmesurado del ancho de banda de Internet y de la red de computadores permitiendo acceso a cualquier dispositivo que se conecte a dicha red.

Así pues, se establece que el mayor riesgo en la institución no proviene de los ataques de afuera sino internamente por parte de los usuarios de las estaciones de trabajo de igual suerte que se evidencia que el manejo de la información no es seguro y que cualquier siniestro puede hacerla irrecuperable.

Por otra parte, en cuanto a las recomendaciones de hardening, respecto de la capa de aplicación no se requieren utilizar todas las medidas posibles, que se quieran o de que se dispongan, esto debido a que, entre más simpleza en la seguridad mejor, ello se sustenta en que al poner demasiadas medidas en este nivel respecto de las estaciones de trabajo habría demasiadas barreras que habría que reconfigurar en caso de poder instalar software nuevo, esto trae a colación el uso de GPO o GPL, las cuales habría que reconfigurar para tal fin sin mencionar el uso de un software reebot and restore que implicaría lo mismo.

Para finalizar, es de poner en relevancia que las medidas en concientización y políticas del modelo de defensa en profundidad (séptima capa) no garantizan que los usuarios harán uso correcto de las medidas tecnológicas, es por eso que es necesario el hecho de implementar barreras a nivel de aplicación (segunda capa), ya que desde allí es mucho más efectiva la protección, esto en razón a que muchas veces cuando una persona hace uso de un bien informático ajeno no le muestra interés por hacer uso adecuado del mismo o protegerlo ya que no pertenece a ella por tanto la implementación del hardening es una labor que se realiza también en contra de la indiferencia de los usuarios informáticos frente al uso de los bienes informáticos ajenos

CONCLUSIONES

- A través del presente proyecto se ha logrado establecer el proceso de defensa en profundidad como una forma de asegurar un sistema informático y su red de computadores, de tal suerte que se puede implementar medidas a libre escogencia en cada una de las capas que componen el modelo.

- Se ha determinado que una buena parte de las soluciones en hardening son basadas en software y en políticas y procedimientos de seguridad, siendo así que el uso de hardware ayuda a perfeccionarlas.

- Se logró detallar y clarificar el concepto de defensa en profundidad de acuerdo al modelo de Microsoft, determinando políticas y procedimientos junto a la seguridad física y lógica para brindar una seguridad más eficiente al interior de una organización.

- En lo que respecta a Windows, se ha identificado como la implementación de hardening ha de implicar medidas específicas para la solución de determinados problemas y que no generen cuellos de botella al instalar varios antivirus, antimalwares o uso de software de mayor complejidad.

- Respecto del uso de GPO y GPL en Windows o Windows Server, se pudo demostrar que brinda una forma efectiva para proteger la configuración de estaciones de trabajo que operen con una serie de aplicaciones básicas y similares en un grupo de trabajo o dominio.

- Se logró poner en relevancia el uso de programas para hardening bajo licencia de uso libre, como también gratuitos o en versiones trial (de prueba) las cuales ayudan a reducir los costos de seguridad informática en una empresa y fomentan de igual manera el uso de freeware al momento de hardenizar sistemas informáticos.

- Frente a Linux y respecto de Ubuntu desktop se estudió y expuso una amplia variedad de herramientas para realizar hardening bajo esta plataforma la cual se puede convertir en un bastión de seguridad en un sistema informático.

- Se puso en relevancia el uso de aplicaciones móviles para el proceso de hardenizado atendiendo a las necesidades de actualidad tecnológica y búsqueda de nuevos métodos de seguridad.

- A través de los resultados arrojados por el análisis de vulnerabilidades a la institución COTEL-Tunja, se logró demostrar una serie de problemas que son comunes a toda empresa pero que pueden ser solucionados aplicando un proceso metódico para la solución de los mismos como es el modelo de defensa en profundidad de Microsoft

- Frente los problemas de seguridad informática de COTEL-Tunja, se ha logrado establecer que una buena parte provienen de la inadecuada configuración de los equipos computaciones y de redes de comunicaciones, de igual manera son generados también por la inadecuada manipulación por parte de los usuarios finales de los mismos

DIVULGACION

La divulgación del presente proyecto se realizará por dos medios, el primero de ellos es realizando una reunión en la institución COTEL de Tunja en la cual estarán presentes los directivos de la misma, en ella se les expondrá los resultados de este proyecto, como podrán implementar las medidas sugeridas y los costos de las mismas, esta reunión será posterior a la aprobación del proyecto por los jurados evaluadores de la especialización en seguridad informática de la UNAD, de tal suerte que contemple las correcciones pertinentes.

El segundo medio de divulgación es el repositorio de la UNAD en donde el proyecto podrá ser revisado por la comunidad académica de la universidad, así como la sociedad en general.

BIBLIOGRAFIA

SANCHEZ, Z. (2011). Desarrollo de una guía para selección y endurecimiento (hardening) de sistemas operativos para un centro de datos. {En línea} {20 de abril de 2016} Disponible en: http://tesis.ipn.mx/jspui/handle/123456789/8466

BALTAZAR, J. (2011). Diseño e implementación de un esquema de seguridad perimetral. Para redes de datos caso práctico: dirección general del colegio ciencias y humanidades. {En línea} {20 de abril de 2016}. Disponible en: http://132.248.9.195/ptb2011/mayo/0669103/0669103_A1.pdf

COLOMBIA. MINISTERIO DE EDUCACION. (2016). Educación para el Trabajo y el Desarrollo Humano - Definición. {En línea} {20 de abril de 2016} Disponible en: http://www.mineducacion.gov.co/1759/w3-article-234968.html

VIEITES, A. (2014). La lucha contra el ciberterrorismo y los ataques informáticos. {En línea} {20 de abril de 2016} Disponible en: http://www.edisa.com/wp-content/uploads/2014/08/La_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

WIKIPEDIA. (2016). Bastion host. {En línea} {27de abril de 2016} Disponible en: https://es.wikipedia.org/wiki/Bastion_host

TARLOGIC. (2016). Bastionado de sistemas (hardening). {En línea} {28 de abril de 2016} Disponible en: https://www.tarlogic.com/servicios/bastionado-de-sistemas-hardening/

MARTÍNEZ, L. (2009). ¿Nos expresamos correctamente? {En línea} {28 de abril de 2016} Disponible en: http://www.securitybydefault.com/2009/11/nos-expresamos-correctamente.html

CARRILLO, A. (2014), análisis y diagnóstico de la seguridad informática de Indeportes Boyacá. {En línea} {29 de abril de 2016} Disponible en: http://repository.unad.edu.co/bitstream/10596/2692/5/53070244.pdf

MARTÍNEZ, L. (2015). La importancia del bastionado de sistemas. {En línea} {29 de abril de 2016} Disponible en:

https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/importancia_bastionado_sistemas

GRAMMATECH. (2016). Software Hardening. {En línea} {29 de abril de 2016} Disponible en: https://www.grammatech.com/software-hardening

SEGURIDAD SyR. (2016). Bastionado de sistemas y servidores. {En línea} {5 de mayo de 2016} Disponible en: https://seguridad.syr.es/servicios-seguridad-informatica/bastionado-de-sistemas-y-servidores

SENA, L. (2004). Introducción a riesgo informático. {En línea} {10 de mayo de 2016} Disponible en http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf

MIFSUD, E. (2012). MONOGRÁFICO: Introducción a la seguridad informática – Amenazas. {En línea} {12 de mayo de 2016} Disponible en http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=5

SYMANTEC. Glosario de Seguridad 101 (2016). {En línea} {15 de mayo de 2016} Disponible en https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

INFORMÁTICA-HOY. (2016). Que es un Firewall y cómo funciona. {En línea} {18 de mayo de 2016} Disponible en: http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Firewall-y-como-funciona.php

SAIVE, R. (2013). 25 Hardening Security Tips for Linux Servers. {En línea} {20 de mayo de 2016}Disponible en: http://www.tecmint.com/linux-server-hardening-security-tips/

DRAGON. (2008). Que es el Hardening Linux con grsecurity. {En línea} {21 de mayo de 2016}Disponible en: http://www.dragonjar.org/hardening-linux-con-grsecurity.xhtml

GARZON PADILLA, G. (2015). Propuesta para la implementación de un sistema de detección de intrusos (IDS) en la Dirección General Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC “pidsinpec”. {En línea} {22 de mayo de 2016} Disponible en http://hdl.handle.net/10596/3494

CISCO. (2016). Cisco IDS 4215 Sensor. {En línea} {25 de mayo de 2016}Disponible en: http://www.cisco.com/c/en/us/support/security/ids-4215-sensor/model.html

CISCO. (2016). Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Module. {En línea} {25 de mayo de 2016} Disponible en: http://www.cisco.com/c/en/us/products/interfaces-modules/catalyst-6500-series-intrusion-detection-system-idsm-2-services-module/index.html

CISCO. (2016). Cisco FirePOWER 8000 Series Appliances. {En línea} {25 de mayo de 2016} Disponible en: http://www.cisco.com/c/en/us/products/security/firepower-8000-series-appliances/index.html

CISCO. (2016). ¿Qué es un firewall? {En línea} {25 de mayo de 2016} Disponible en: http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

WATCHGUARD. (2016). Firewall de nueva generación (NGFW). {En línea} {26 de mayo de 2016} Disponible en: http://www.watchguard.com/es/wgrd-international/products/ngfw/overview

NORMAS9000. (2016). ¿Qué es ISO 9001:2008? {En línea} {27 de mayo de 2016} Disponible en: http://www.normas9000.com/que-es-iso-9000.html

UNAD. (2016). 233003 Sistema de gestion de la seguridad de la información sgsi - Inventario de Activos. {En línea} {27 de mayo de 2016} Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321_paso_1_inventario_de_activos.html

ROS, I. (2014). Windows Defender es el peor antivirus, según AV-Test. {En línea} {28 de mayo de 2016} Disponible en: http://www.muycomputer.com/2015/03/26/windows-defender-peor-antivirus

PERGAMINOVIRTUAL. (2015). Definicion de Backdoor. {En línea} {29 de mayo de 2016} Disponible en: http://www.pergaminovirtual.com.ar/definicion/Backdoor.html
Ecured. (2016). Bastion Host. 2016, de ecured.cu Disponible en: https://www.ecured.cu/Bastion_Host

SUNDSTROM, K. (2014). ¿Qué es una estación de trabajo de computadora? {En línea} {30 de mayo de 2016} Disponible en: http://www.ehowenespanol.com/estacion-computadora-hechos_400522/

SEGURIDADPC. (2016). Concepto de exploit. {En línea} {30 de mayo de 2016} Disponible en: http://www.seguridadpc.net/exploit.htm

TECHOPEDIA. (2016). Hardening. {En línea} {30 de mayo de 2016} Disponible en: https://www.techopedia.com/definition/24833/hardening

QUEES. (2016). ¿Qué es parchear?. {En línea} {30 de mayo de 2016} Disponible en: http://quees.la/parchear/

DEFINICIONABC. (2016). Definición de Seguridad informática. {En línea} {30 de mayo de 2016} Disponible en: http://www.definicionabc.com/tecnologia/seguridad-informatica.php

CULTURACION. (2016). ¿Qué es un sniffer? {En línea} {30 de mayo de 2016} Disponible en: http://culturacion.com/que-es-un-sniffer/

UNAD. (2016). Lección 1: Conceptos de Vulnerabilidad, Riesgo y Amenaza. 2{En línea} {30 de mayo de 2016} Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

CISCO. (2016). WLAN. {En línea} {30 de mayo de 2016} Disponible en: http://www.cisco.com/c/es_es/solutions/mobility/WLAN.html

GUTIERREZ, A. (2015). WEP o WPA para proteger tu red Wi-Fi. {En línea} {30 de mayo de 2016} Disponible en: http://windowsespanol.about.com/od/RedesYDispositivos/a/Wep-O-Wpa-Para-Proteger-Tu-Red-Wi-Fi.htm

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273 de 2009 (2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado “de la protección de la información y de los datos” – denominado. {En línea} {30 de mayo de 2016} Disponible enhttp://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 599 de 2000 (2000). Por la cual se expide el Código Penal. {En línea} {30 de mayo de 2016} Disponible enhttp://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

MENDEZ, C. (2001). Metodología, Diseño y Desarrollo del Proceso de Investigación. Colombia. p.136.

HEREDIA, M. S. (2009). METODOLOGÍA DE LA INVESTIGACIÓN. {En línea} {30 de mayo de 2016} Disponible en: http://www.monografias.com/trabajos58/metodologia-investigacion/metodologia-investigacion2.shtml

MEDINA, M. C. (2010). TIPOS DE INVESTIGACIÓN. {En línea} {30 de mayo de 2016} Disponible en: http://www.monografias.com/trabajos59/tipos-investigacion/tipos-investigacion.shtml

HARRISON, R. (Guía de defensa en profundidad antivirus). 2004. {En línea} {8 de octubre de 2016 } Disponible en: https://technet.microsoft.com/es-es/library/cc162791.aspx

TORREZ, L. (2010). ¿Qué es Honeynet? {En línea} {19 de octubre de 2016} Disponible en: http://aiturrih.blogspot.com.co/2010/11/que-es-honeynet.html

AUDITORIADESISTEMASCONTADURIAUCC. (2012). Técnicas de auditoria asistidas por computadoras. {En línea} {4 de noviembre de 2016} Disponible en: http://auditoriadesistemascontaduriaucc.blogspot.com.co/2012/06/tecnicas-de-auditoria-asistidas-por.html

OROVENGUA, J. (2015) {En línea} {5 de noviembre} Disponible en http://www.linux-party.com/index.php/35-linux/8634-recuperar-la-contrasena-de-root-en-linux-o-hackear-tu-propio-sistema

JOAN. (2015). Tu propio IDS con Snort y Snorby en Linux Debian 7. {En línea} {10de noviembre} Disponible en: https://www.joanesmarti.com/tu-propio-ids-con-snort-y-snorby-en-linux-debian-7/

CISOFY. (2016). Lynis. {En línea} {14 de noviembre de 2016} Disponible en: https://cisofy.com/lynis/

UPADHYAY, R. (2016). How to Install Snort NIDS in Ubuntu 15.04? {En línea} {18 de noviembre de 2016} Disponible en: https://www.unixmen.com/install-snort-nids-ubuntu-15-04/

ATTIQUE, M. (2015). Install and Configure Snort HIDS with Barnyard2, Base & MySQL on Ubuntu. {En línea} {18 de noviembre de 2016} Disponible en: http://blog.muhammadattique.com/install-configure-snort-hids-barnyard2-base-mysql-ubuntu/

ANEXO A. AUDITORIA LYNIS

EJEMPLO DE AUDITORÍA DE SERVIDOR UBUNTU DESKTOP 16.04

En este caso se hará auditoria del computador destinado a monitorizar la red del instituto COTEL-TUNJA, con el sistema operativo Ubuntu, dicho computador ha sido recién instalado, por tanto, carece de instalación de paquetes completos (ya sea el caso de apache2, mysql, u otros), la idea de ello es mostrar que a pesar de que es un sistema operativo Linux, igual presenta una serie de vulnerabilidades que pueden ser aprovechadas más aún si él configuraciones por defecto. En ese sentido lo primero que se hará es instalar Lynis para verificar el estado actual en cuanto a seguridad.

Para entender mejor el análisis que arroja este programa es necesario tener en cuenta las descripciones que nos brinda de tal suerte que nos indicará a través de una serie de advertencias del estado de determinado elemento del sistema de la siguiente manera:

Color rojo: el elemento no está instalado o no está bien configurado debidamente y por tanto es un riesgo (Warning, Not installed, Different)

Color verde: el elemento está presente o está correctamente instalado y/o configurada (Found, Done, OK)

Color amarillo: elemento que se sugiere reconfigurar o reinstalar, o por otro lado puede ser desconocida su procedencia; no obstante, esto no afecta de forma importante la seguridad sistema (Suggestion, Unkown)

Color blanco: el elemento no está habilitado o no se ha encontrado (not found, not enabled)

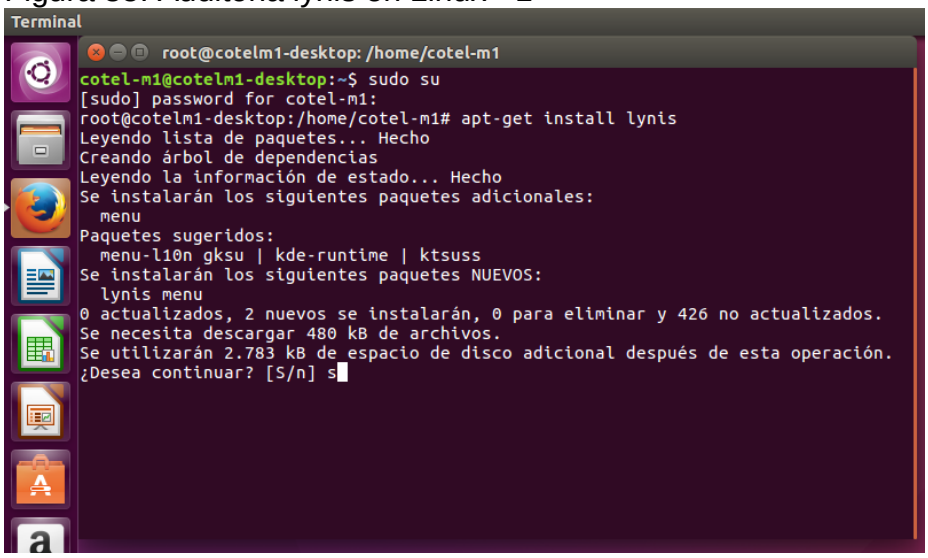
Herramienta de auditoria: Lynis
Equipo: cotel-m1

Descripción:

Como se observa en la siguiente figura se instala el programa Lynis a través del repositorio de Ubuntu

apt-get install lynis

Figura 35. Auditoria lynis en Linux - 1



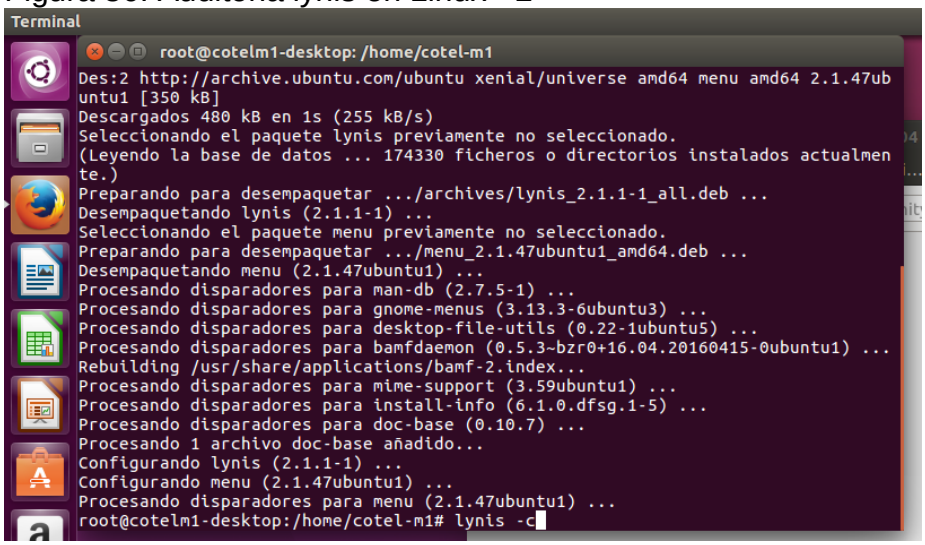
Fuente: el autor

Una vez que el programa ha sido instalado para poder utilizarlo se ejecuta el comando

lynis –c

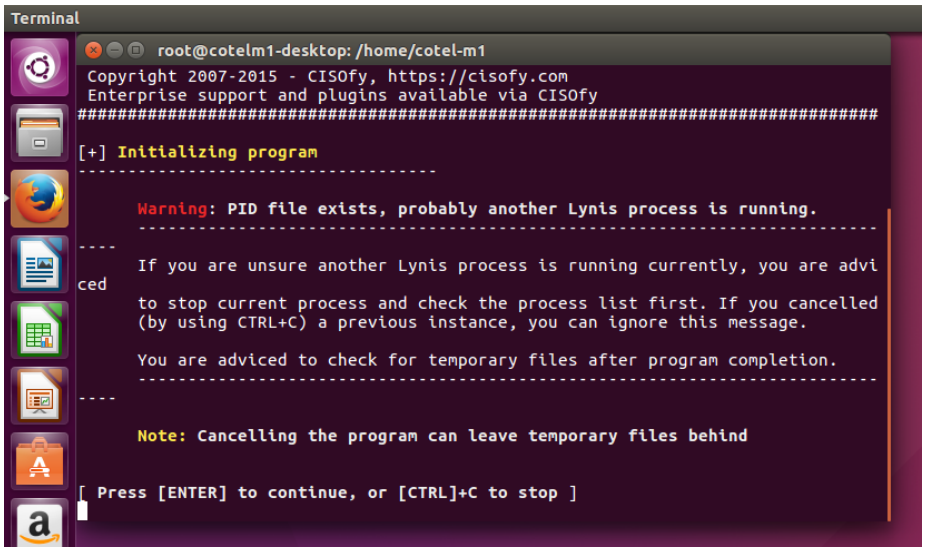
Esto permitirá hacer un escaneo completo del sistema

Figura 36. Auditoria lynis en Linux - 2



Fuente: el autor

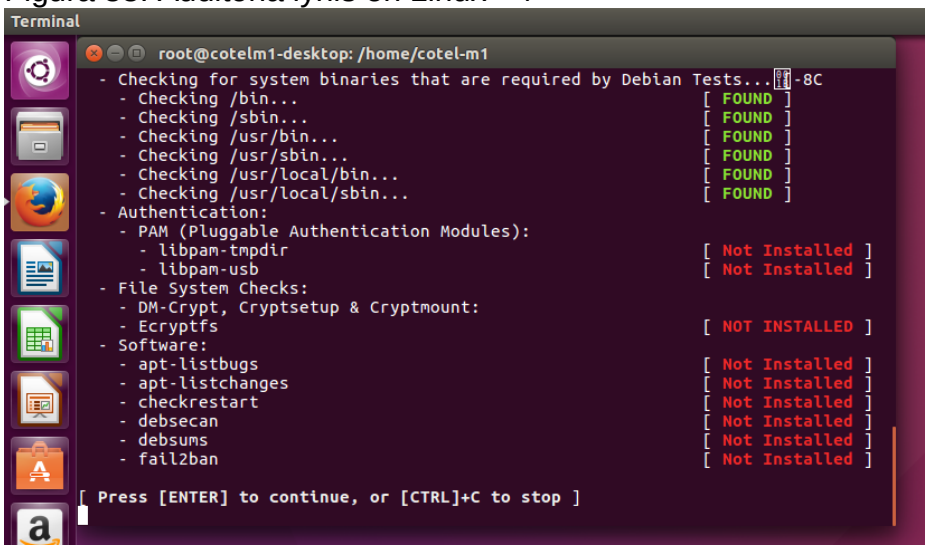
Figura 37. Auditoria lynis en Linux - 3



Fuente: el autor

Una vez que es ejecutado empieza a obtener los primeros resultados de cada análisis, en este caso caso se observa que falta la instalación de los siguientes complementos: módulos de autentificación (authentication), Sistema de verificación de archivos (file check system) y software (referente a listas de cambios y errores de otros)

Figura 38. Auditoria lynis en Linux - 4



Fuente: el autor

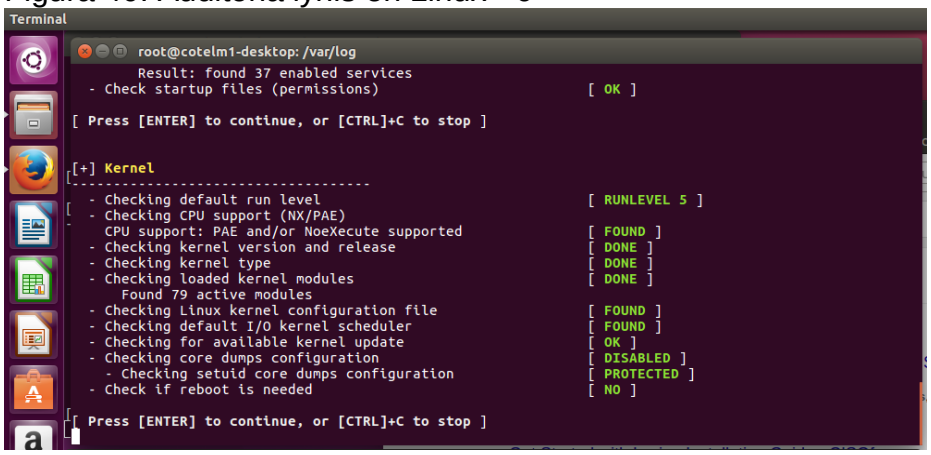
En la siguiente imagen en la opción de “arranque y servicios” (boot y services) se puede apreciar un error importante o advertencia del cual se marca como “warning”, en este caso es el de la contraseña (password) sistema la cual se dejo con una extensión muy corta por tanto hay que cambiarla por una que sea más larga y segura.

Figura 39. Auditoria lynis en Linux - 5

Fuente: el autor

La sección kernel (núcleo) como se observa presenta una adecuada configuración en cuanto al núcleo del sistema operativo

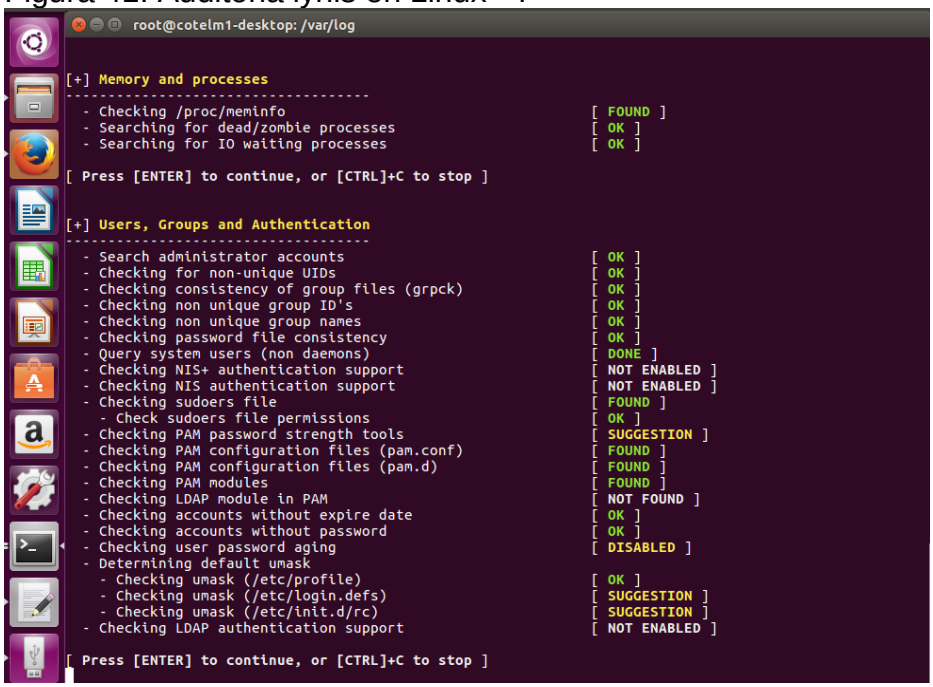
Figura 40. Auditoria lynis en Linux - 6



Fuente: el autor

En sección usuarios, grupos y autentificación (users, groups and authentication) de observar que se recomienda realizar cambios de la configuración de los archivos paswrod strenght tools y aging, igualmente para determinado por defecto de umask (determining defalt umask)

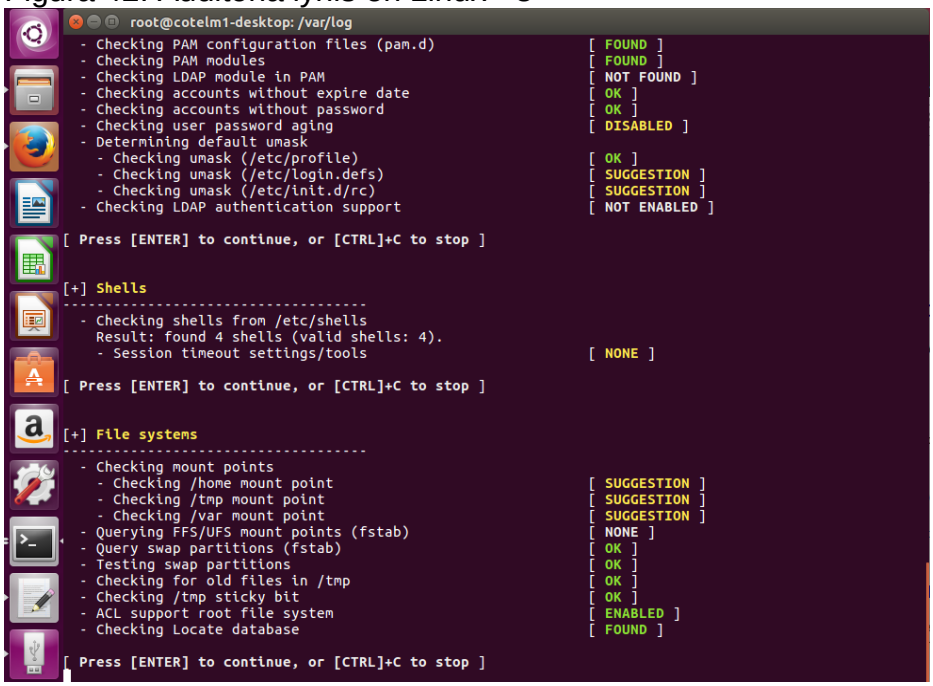
Figura 41. Auditoria lynis en Linux - 7



Fuente: el autor

En la sección de archivos del sistema, se marcan como sugerencia los puntos de montaje de los directorios (home, tmp y var) esto ya que es una recomendación de seguridad habitual en Linux el separar por particiones el directorio home, tmp y var así como también el de usr, tal como se hace con la partición swap.

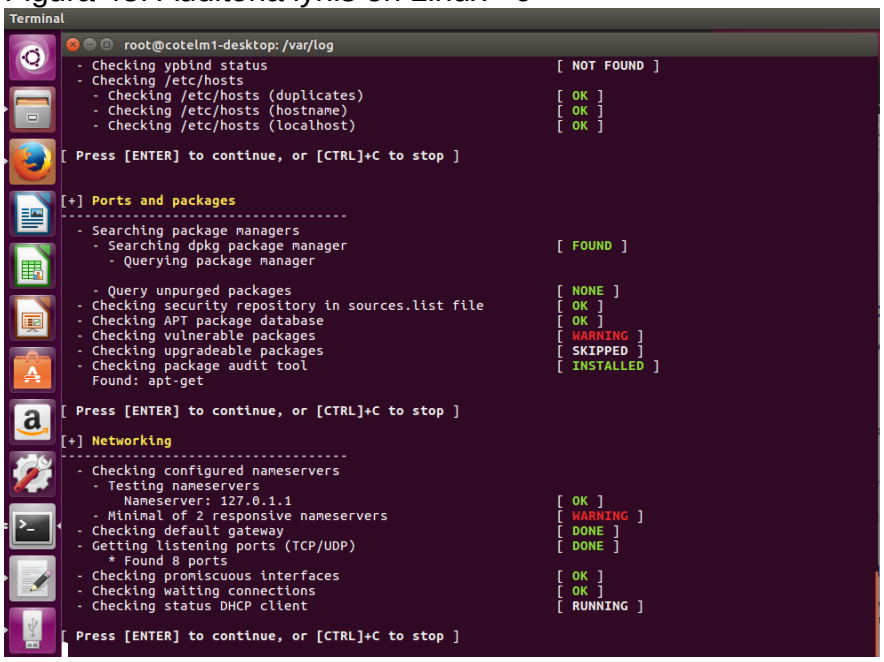
Figura 42. Auditoria lynis en Linux - 8



Fuente: el autor

En la sección de puertos y paquetes (ports and packages), se podrá apreciar que hay una advertencia en cheking vulnerable packages, implica realizar configuraciones de seguridad para verificar la procedencia de los paquetes desde los repositorios a los que esté apuntando el sistema. Igualmente en la sección

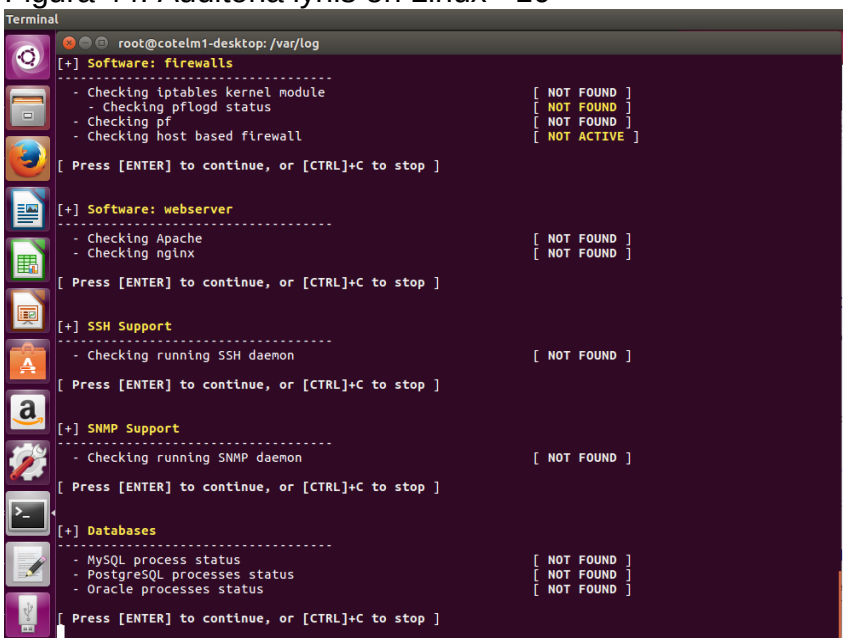
Figura 43. Auditoria lynis en Linux - 9



Fuente: el autor

En la sección de firewall (cortafuegos) se puede apreciar que éste no está configurado y se marca como una recomendación en amarillo, no obstante esta debería ser el rojo ya que para igual es una barrera importante seguridad en el sistema y la cual debe ser implementada (esto a través de ufw e iptables)

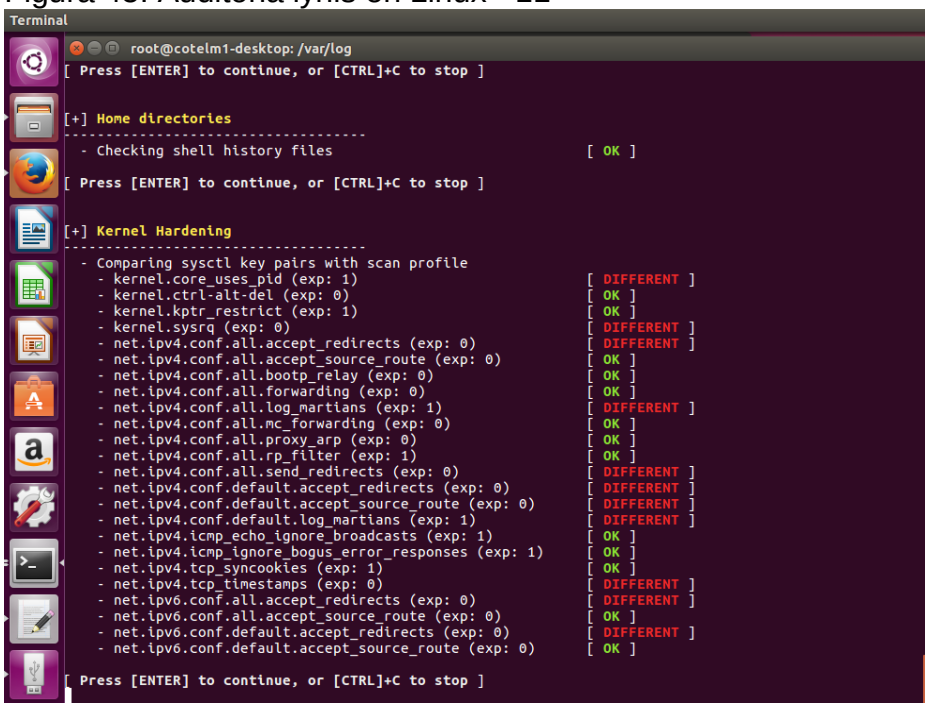
Figura 44. Auditoria lynis en Linux - 10



Fuente: el autor

En la siguiente pestaña se puede apreciar que hay una serie de no conformidades respecto de las configuraciones del núcleo del sistema como tal como también algunas que apuntan a la configuración del protocolo IPV4 e IPV6, lo recomendado en esta situación es actualizar el núcleo del sistema y desactivar el uso de IPV6.

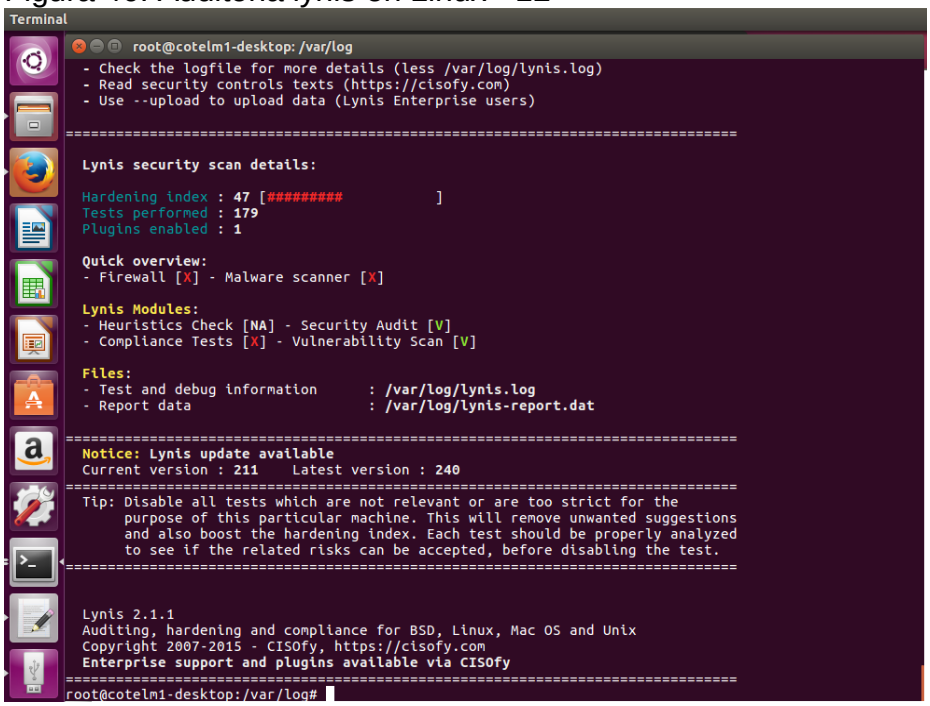
Figura 45. Auditoria lynis en Linux - 11



Fuente: el autor

Luego que el programa ha terminado el análisis de auditoría este muestra en donde se puede poder ver el resumen o reporte de la misma, en este caso hay que ir a **var/log.** Vale resaltar que al final del escaneo en la línea azul que dice Hardeing index: 47; este indicador es el porcentaje de seguridad sistema en ese momento en ese sentido corresponde a un 47% de seguridad, obviamente si se aplican las medidas correctivas sobre las advertencias o sugerencias que menciona el programa este indicador aumentará.

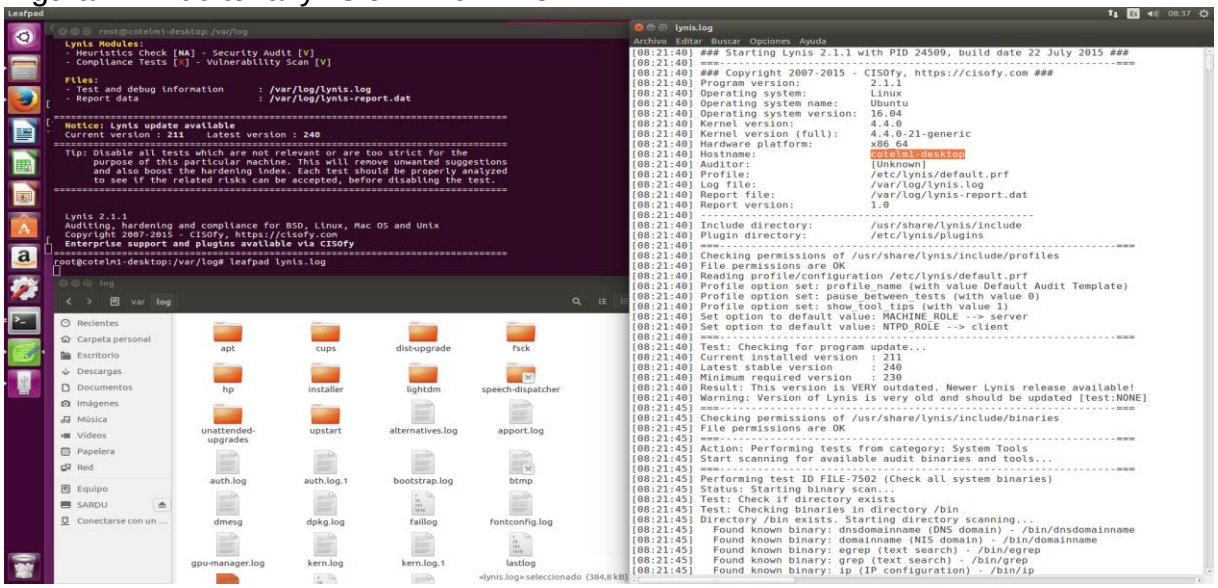
Figura 46. Auditoria lynis en Linux - 12



Fuente: el autor

En este caso se usó el editor de texto leafpad para abrir el reporte que se ha generado

Figura 47. Auditoria lynis en Linux - 13



Fuente: el auto

ANEXO B. RAE

RAE

Fecha de Realización: 6/12/2016
Título: ESTUDIO SOBRE LA APLICACIÓN DE HARDENING PARA MEJORAR LA SEGURIDAD INFORMÁTICA EN EL CENTRO TECNICO LABORAL DE TUNJA – COTEL
Autor: FACHE, Jaison
Palabras Claves: Amenaza informática, hardening, bastionamiento, Firewall, antivirus, defensa en profundidad, Linux, windows, sniffer, TAAC, Vulnerabilidad informática, WLAN, WPE, WPA
Descripción: monografía de estudio sobre la implementación de técnicas y medidas en hardening teniendo como referencia los sistemas operativos Windows y la Linux como propuesta para la solución de problemas de seguridad informática del Instituto COTEL de Tunja
Fuentes: SANCHEZ, Z. (2011). Desarrollo de una guía para selección y endurecimiento (hardening) de sistemas operativos para un centro de datos. Disponible en: http://tesis.ipn.mx/jspui/handle/123456789/8466 VIEITES, A. (2014). La lucha contra el ciberterrorismo y los ataques informáticos. Disponible en: http://www.edisa.com/wp-content/uploads/2014/08/La_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf TARLOGIC. (2016). Bastionado de sistemas (hardening). Disponible en: https://www.tarlogic.com/servicios/bastionado-de-sistemas-hardening/ MARTÍNEZ, L. (2015). La importancia del bastionado de sistemas. Disponible en: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/importancia_bastionado_sistemas GRAMMATECH. (2016). Software Hardening. Disponible en: https://www.grammatech.com/software-hardening

SEGURIDAD SyR. (2016). Bastionado de sistemas y servidores. Disponible en: https://seguridad.syr.es/servicios-seguridad-informatica/bastionado-de-sistemas-y-servidores

Contenido del documento:

El hardening o bastionamiento se define como el proceso de proteger de un sistema o conjunto de sistemas informáticos mediante la aplicación de configuraciones de seguridad específicas para prevenir ataques informáticos; dicho proceso puede abarcar desde medidas en software dependiendo del sistema operativo que manejen las estaciones de trabajo, así como también medidas en hardware que ayudan a proteger la periferia del sistema y su red en términos físicos.

Así entonces, con el presente trabajo se pretende dar a conocer en detalle lo que es el hardening su aplicabilidad, ventajas, estrategias y técnicas del mismo, a la vez que se reconocerá la importancia del modelo defensa en profundidad promovido por Microsoft y se describirán las capas que lo componen de tal suerte que a partir de las mismas se puedan identificar las falencias en seguridad informática que presenta el Instituto COTEL de Tunja y proponer soluciones respecto de los estas.

Para ello se presentarán herramientas y medidas de hardening en estaciones de trabajo tipo Windows como el caso de Snort (IDS), WinAudit (TAAC), software Reboot Restore, bloqueo a través del archivo hosts y aplicación políticas de seguridad en Windows y Windows server.

Igualmente se hará hincapié en la identificación herramientas y medidas de hardening para estaciones de trabajo basadas en ambientes Linux a través del reconocimiento de características de Lynis, OpenVAS y snort, así como también la implementación de un Inicio de sesión con verificación de dos pasos; todo lo anterior alrededor de Linux Ubuntu desktop.

Por último, se plantea el realizar una propuesta de hardening para el Instituto COTEL de Tunja a partir de los hallazgos encontrados en un análisis preliminar de vulnerabilidades de acuerdo a modelo de defensa en profundidad.

Metodología: Esta investigación sigue una estructura basada en un estudio descriptivo, identificando antecedentes y referencias respecto del tema seleccionado como objeto de estudio (hardening). Los métodos a utilizar en esta investigación serán análisis y síntesis, y Las fuentes primarias para este estudio serán aquellos contenidos referentes al hardening que se encuentren en tesis, monografías, así como artículos de internet. Respecto de la población estará constituida por la comunidad administrativa y estudiantil del instituto COTEL-TUNJA. Frente a metodología de desarrollo se establecieron 4 objetivos a desarrollar los cuales son: 1. conceptos teóricos de hardening y modelo de defensa en profundidad promovido por Microsoft 2. Medidas de hardening en Windows 3. Medidas de hardening en Linux teniendo como referencia Ubuntu desktop; y 4. Generación de una propuesta de hardening COTEL-TUNJA de acuerdo al modelo de defensa en profundidad promovido por Microsoft.
Conceptos nuevos: hardening, hardenizado bastionamiento, bastionar.
Conclusiones: El realizar un modelo de defensa en profundidad y proponer medidas de seguridad respecto de este no quiere decir que con ello se reemplaza otros métodos de seguridad como un SGSI (el cual es más explícito en las medidas que se aplican) sino que a través del método de defensa en profundidad se presenta una forma de asegurar un sistema informático y su red de computadores de una forma eficaz toda vez que se carezca de tiempo y/o recursos financieros, de tal suerte que se pude implementar medidas a libre escogencia en cada una de las capas que componen el modelo.
Autor: JAISON DUVANY FACHE MONTAÑA