ROBUSTECIMIENTO DE SEGURIDAD RED LAN CORPORATIVA

JORGE GUILLERMO CASTRO MALDONADO

UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA.

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA D.C

2018

ROBUSTECIMIENTO DE SEGURIDAD RED LAN CORPORATIVA

JORGE GUILLERMO CASTRO MALDONADO

PROYECTO DE EMPRENDIMIENTO EMPRESARIAL

SALOMON GONZALEZ

DIRECTOR DEL CURSO PROYECTO DE GRADO II.

UNAD

ESCUELA DE CIENCIAS BÁSCIAS, TECNOLOGÍA E INGENIERÍA.

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA

2018

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D.C, 04 de Diciembre del 2018

AGRADECIMIENTOS

Dedico este proyecto de grado de Seguridad Informática en la cual se plantea un sistema de gestión de seguridad informática en una empresa de origen estadounidense al director del curso al brindarme la oportunidad de modificar y a la vez perfeccionar el presente proyecto, el cual puede ser utilizado y amoldado para cualquier compañía que esté interesada en implementar un proyecto y/o sistema de gestión de seguridad informática en su organización.

CONTENIDO

Pag.

LISTA DE GRAFICAS

Pag

LISTA DE TABLAS

Pag

INTRODUCCIÓN.

El Presente trabajo plantea las mejores prácticas en lo que refiere al robustecimiento de una red LAN corporativa de cualquier organización, se enfoca en tomar desde lo más elemental como lo es la seguridad en la BIOS de los equipos de computa hasta soluciones avanzadas tipo WebApplication Firewall.

Estas buenas prácticas tienen un orden específico el cual se basa en el modelo OSI esto referente a networking, debido a que si se parte desde la primera capa la cual es la capa física, siguiendo por enlace de datos, red, transporte, sesión, presentación y finalizando en la capa de aplicación; cada una de las mismas tiene ítems puntuales en los cuales se puede llegar a realizar cualquier ataque con la intención de vulnerar la información que refiere a la capa específica.

Este proyecto se plantea en una topología simple, en la cual se encuentra la LAN en layer 2, servidores en la misma capa y en una tercera y cuarta capa servicios de aplicación, volviendo a layer 7 a nivel de software inteligente y/o plugins para control de contenido, esto por medio de una consola EPO.

RESUMEN

El presente trabajo se encarga de plasmar por las propias palabras del autor, basado en su experiencia y documentado en buenas prácticas en lo referente a lo que comprende la seguridad informática de una organización genérica, la cual busca realizar un robustecimiento en la seguridad LAN de su red empresarial, partiendo desde lo más básico y sencillo como lo es la seguridad en los PC y Networking hasta soluciones inteligentes tipo WAF y software en capa de aplicación (modelo OSI).

Este documento sugiere las buenas prácticas las cuales pueden ser tomadas en cuenta si no es en su totalidad, ya que cada organización es diferente en cuento a sistemas de información, pero si puede tomarse las secciones y/o soluciones sugeridas las cuales de manera casi que genérica están al alcance de una compañía que no desee invertir mucho dinero y esfuerzo en la misma.

GLOSARIO

ANÁLISIS DE VULNERABILIDADES: Esta es la manera por la cual se realiza de manera remota, ya sea con técnica caja negra, caja gris o caja blanca una inspección a cada una de las instancias a analizar logrando detectar fallos y/o falencias a nivel de seguridad informática en las mismas. Este análisis de vulnerabilidad solo imprimirá las falencias más no hará intrusión a nivel de capa 7.

INTRUSIÓN(ES): Este concepto a nivel de seguridad informática refiere a una vez realizado un análisis de vulnerabilidad y detectado las fallas de las paliaciones, se procede a realizar una explotación a las mismas, en otras palabras una intrusión.

DoS: Denegación de servicio; es la técnica por la cual se realiza un ataque masivo a un servicio y/o instancia y se logra sobre saturar a la misma con tal de realizar una caída general del servicio.

SQL Injection: Técnica de intrusión a nivel de sentencias de SQL a base de datos a una aplicación, lo cual se considera código intruso.

WAF: Web Application Firewall, es un dispositivo el cual puede ser un Appliance o un Software el cual analiza tráfico web proveniente de la WAN y protege la instancia o Web Service de distintos ataques previniendo ataques tipo ROBOT, u otros tipos de ataques tipo SQL Injection, Cross Site Scripting, entre otros.

FIREWALL: Dispositivo de seguridad perimetral en una red quien se encarga del enrutamiento y primer nivel de protección de la LAN desde la WAN.

IPTABLES: Se puede considerar como un firewall a nivel de capa 7 de los servidores bajo entorno UNIX. Aplica tres reglas las cuales son: IMPUT, OUTPUT y FORWARD.

SELINUX: Security-Enhanced Linux, es un módulo de seguridad del kernel LINUX el cual proporciona mecanismos de políticas de seguridad en torno a control de acceso.

ATAQUES DE TIPO ROBOT: Su abreviación en el mundo de la seguridad informática es Botnet, el cual es un término que refiere a un conjunto o redes de robots informáticos (bots) que se ejecutan de manera automática, coordinada y

autónoma para realizar ataques y/o explorar vulnerabilidades de sistemas informáticos.

CROSS SITE SCRIPTING: La vulnerabilidad de Cross Site Scripting (XSS por sus siglas en inglés) permite aprovecharse de las falencias en el filtrado de caracteres especiales e instrucciones enviados a las aplicaciones que posteriormente son reflejados en los navegadores de las víctimas, permitiendo el robo de las sesiones de usuario e información confidencial.

1. FORMULACIÓN DEL PROBLEMA

En la actualidad poco a poco se ha venido tomando conciencia de la importancia que refiere el robustecer la seguridad informática y de la información en las compañías sin importar su tamaño, yendo desde las más grandes pasando por las medianas y terminando en las pequeñas; cada una de estas acorde a su presupuesto destinado y/o prioridad del negocio. Este proceso aunque se va dando de manera progresiva y se puede decir que casi a medida que van saliendo nuevos ataques masivos y/o mundiales de virus como el último ataque mundial llamado Wanna Cry tipo ransomware.

Se puede considerar que el robustecimiento de la seguridad informática de las organizaciones está directamente relacionado con las prioridades del negocio y este a un presupuesto establecido para el mismo, cada organización establece un protocolo o cierto requerimiento a cumplir en esta labor y este de cierta manera acotado a lo que se requiere, pero aun así hay ítems minúsculos los cuales puedes ser explotados por malwares, un ejemplo claro es que la mayoría de organizaciones no tienen establecido sistemas de actualización automáticas tipo WSUS (Windows System Update Services) que se encargan de realizar actualizaciones en OU (Unidades Organizativas) por medio de GPO (Políticas de grupo), esta fue una vulnerabilidad que aprovechó de manera satisfactoria el Wanny Cry para diseminarse tipo gusano informático en España.

Este proyecto de seguridad informática planea establecer buenas prácticas basadas en el modelo OSI para el robustecimiento de una LAN corporativa de una organización en general, partiendo desde la capa física como bien lo enuncia este modelo hasta la capa de aplicación, enfocada en sistemas de seguridad inteligente tipos EPO de Consolas Antivirus. Para sistemas de publicación de tipo WebService con consumo FQDN también se plantean buenas prácticas de topologías basadas en firewalls perimetrales y Web Application Firewall con tal de detectar ataques de tipo netboot.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Definir un plan en lo referente al robustecimiento de seguridad en una red LAN corporativa.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar acorde al modelo OSI, mejoras en robustecimiento de la red LAN en cada una de sus capas comprendidas.
- Realizar proceso de análisis en cuanto a las vulnerabilidades encontradas, para su posterior corrección.
- Establecer buenas prácticas acorde a vulnerabilidades encontradas.

3. ALCANCE

El presente proyecto aplicado en la empresa Mc21 Colombia SAS, brinda de manera clara y explícita la práctica correcta para realizar un robustecimiento de la red LAN corporativa, esto aplicado a cada una de las capas del modelo OSI, el cual se subdivide en capa de host y capa media, logrando así dar soluciones a los equipos y/o elementos que lo componen.

4. MARCO DE REFERENCIA

4.1 MARCO TEÓRICO:

En lo que refiere a un proyecto empresarial orientado al robustecimiento de la red LAN corporativa, se debe plantear esta como una necesidad estratégica de la organización y como objetivo en el fortalecimiento y aseguramiento del activo más importante que se tiene, la cual es su información. De igual manera como pilar del mismo proyecto se debe cumplir con los tres principios que refieren a lo que se considera seguridad de la información los cuales son: Integridad, Confidencialidad y Control de acceso, de tal manera asegurando la continuidad y disponibilidad de sus operaciones y sistemas de información. Todo esto basado en las buenas prácticas para que de tal manera dado el momento de una contingencia reducir al mínimo los años que se puedan llegar a causar.

Un proyecto de robustecimiento de una red LAN corporativa debe obedecer a una política interna de la organización y enfocar sus objetivos a fortalecer y asegurar la continuidad de la operación de igual manera los servicios que prestan los mismos ya sean a cliente interno o cliente externo.

Este proyecto se enfoca en las buenas prácticas para el aseguramiento de una red corporativa basado principalmente en el modelo OSI, ya que este es un modelo de referencia para los protocolos de comunicaciones sobre IP. Iniciando este mismo en la capa física y terminando en la capa de aplicación.

4.2 MARCO LEGAL:

Cada vez que una compañía decide realizar una inversión de tiempo y dinero en mejorar y/o robustecer la seguridad LAN de la misma debe de manera obligatoria cumplir con todas las normas legales, leyes, decretos y demás las cuales se puedan aplicar para el desarrollo de cada una de las actividades contempladas en el proyecto.

A continuación se referencian varias leyes y normatividades las cuales hacen referencia al marco legal en Colombia:

[1]Ley 1273 de 2009:

La cual añade dos nuevos capítulos al Código Penal Colombiano:

- Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;

- Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

[2]Ley 603 de 2000

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

[3]Ley Estatutaria 1266 del 31 de Diciembre del 2008

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

[4]Ley 1273 del 5 de Enero del 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

---

[1] Nivel Nacional, Ley 1273 de 2009, Artículo 1. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[2] Soluciones TIC, Ley 603 de 2000. Disponible en: http://www.e-solucionestic.com/ley-603-del-2000/

[3] Redipd, Ley Estatutaria 1266 del 31 de Diciembre del 2008, Artículo 4° sección B. Disponible en: http://www.redipd.org/legislacion/common/legislacion/Colombia/LEY_1266_31_12_2008_HabeasData_COLOMBIA.pdf

[4] Secretaría Jurídica Distrital, Ley 1273 del 5 de Enero del 2009, Capítulo 1. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[5]Ley 1341 del 30 de julio del 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

[6]Ley 599 de 2000

Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

[7]NORMA ISO/IEC 27001:2013

Estándar internacional que se aplica para la gestión de la seguridad de la información. Al manejar el Sistema de Gestión de Seguridad de la Información SIGI, se busca minimizar los riesgos, para esto se deben establecer procesos y procedimientos que ayuden a la organización a llegar a la excelencia.

4.3 MARCO CONCEPTUAL.

La seguridad informática se compone de los siguientes principios: confidencialidad, integridad y disponibilidad, estos tres principios orientados a un fin en común el cual es garantizar que la información, siendo ésta considerada

[5] MinTIC, Ley 1341 del 30 de julio del 2009. Capítulo 1. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[6] Secretaría Jurídica Distrital, Ley 599 de 2000. Artículo 195. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

[7] 7. Adbisera Expert Solution, NORMA ISO/IEC 27001:2013. Disponible en: https://advisera.com/27001academy/es/que-es-iso-27001/

como el activo más importante de toda empresa no se vea vulnerada y/o afectada por entes externos.

Para una adecuada gestión de la seguridad de la información, en una organización es de vital importancia implementar un plan de robustecimiento de la red, en este caso corporativa basado en buenas prácticas y enfocado en el modelo OSI, este el cual refiere a la manera por la cual se logra subdividir de manera física y a su vez lógica el proceso de comunicación partiendo desde el ente emisor, pasando por el medio y llegando al receptor.

Este proyecto se enfoca a tomar cada una de las capas del Modelo OSI y acorde a su teoría dividirla en dos secciones principales, las cuales son la capa media y capa de aplicación; la capa media refiere a todo lo que comprende networking, permisos a nivel de comunicaciones y seguridad perimetral, la capa de aplicación tal como lo enuncia el modelo OSI se basa en soluciones inteligentes o de software las cuales permiten llegar a un nivel mucho más granular y a su vez específico, logrando compaginar estas dos capas macros del modelo OSI se logra tener una mejora esencial y fundamental en cualquier red corporativa, ya que este proyecto toma en cuenta las buenas prácticas en una red casi de manera genérica y al alcance de cualquier administrador de seguridad informática.

Abajo se describe de manera gráfica las siete (7) capas del modelo OSI y las dos capas macros que la contienen, frente a las mismas la aplicabilidad según las buenas prácticas en las cuales se debe trabajar para el reforzamiento de la misma.

En lo que refiere al ítem específico como Análisis de Vulnerabilidad se encuentra este en las dos capas, ya que el primer paso para realizar una validación de la seguridad de una red es partiendo desde las capas de red; en este caso las tres primeras, y posteriormente a estas si se logra detectar alguna falla p falencia en la configuración los siguientes accesos toman la capa de aplicación.

Grafica 1. Marco conceptual.

Fuente: El Autor.

5. DISEÑO METODOLOGICO.

5.1 Metodología de Desarrollo

El objetivo principal del robustecimiento de una red LAN corporativa en sí es el mejorar la calidad de vida de todas las personas que trabajan en una empresa u organización, ya que de manera proactiva en vez de reactiva y basada en buenas prácticas se plantea el llevar un orden, un orden a nivel de ingeniería basados en el modelo OSI. Modelo que se toma de manera jerárquica, física y a su vez lógica el paso de información partiendo desde la capa física; en este caso equipos de cómputo de los usuarios finales hasta la capa de aplicación la cual refiere a los servicios consumibles por parte de los usuarios finales.

En este caso basado en el PMI, se planteará el proyecto de robustecimiento de una red LAN Corporativa bajo los lineamientos y ejecución de la gestión de proyectos, basados en las siguientes fases de proyecto PMI:

- Inicio.
- Planificación.
- Ejecución.
- Monitoreo y Control
- Cierre.

El presente proyecto llamado robustecimiento de seguridad red LAN corporativa, al ser comprendido y ejecutado en la empresa Mc21 Colombia SAS es de vital importancia poner en constancia la aprobación de la empresa misma, en la cual consta no solo el interés de la empresa en desarrollar este proyecto sino también comprende los costos del mismo así como la importancia que comprende este para el correcto funcionamiento de su infraestructura tecnológica.

Por lo tanto se inserta en la siguiente imagen la carta solicitada a la gerencia de tecnología quien realiza la aprobación de la misma por la presidencia de la compañía.

Grafica 2: Carta de solicitud para proyecto.

mc21 COLOMBIA	FORMATO	CODIGO: SOL-GT-FT-12
	SOLICICITUD A PRESIDENCIA REQUERIMIENTOS NUEVOS	VERSION: 01

Presentado por	Ing. Guillermo Castro	Reviso por	Alejandro Murillo
Cargo	Coordinador de Infraestructura	Cargo	Gerente de Ingeniería y tecnología

Fecha:	14 de Junio del 2016
Lugar:	Bogotá
Tipo de Solicitud:	Proyecto de Seguridad Informática
Nombre de proyecto, si aplica:	ROBUSTECIMIENTO DE SEGURIDAD RED LAN CORPORATIVA.
Impacto de la empresa:	Mejora y aseguramiento de su infraestructura tecnológica.
Breve descripción:	Debido a los varios ataques y vulneraciones tanto a nivel interno como a nivel externo, se necesita realizar un plan de robustecimiento de la red local corporativa, el cual comprenda varios ítems partiendo desde los equipos de cómputo hasta los servidores, ya sean los que son para uso de cliente interno y los servidores que son uso externo tipo webservices .
¿Porque es necesario?	De no realizarse un robustecimiento corporativo en la organización estaría la misma vulnerable no solo a nivel interno, en el caso de los propios usuarios de la compañía, sino también por múltiples ataques realizados a los web services, entre los cuales se han detectado escaneos de puertos, intentos de intrusiones, cross site scripting, ataques de denegación de servicio, entre otros.

Se aprueba:

Sí [X] No [ ]

Quien aprueba: Piedad Pineda.

Cargo: Presidenta.

Firma: Piedad Pineda

Fuente: El autor.

De igual manera como se envió a la presidencia el proyecto de robustecimiento a la red LAN corporativa para Mc21 Colombia SAS, se inserta de igual

manera la imagen correspondiente a la respuesta de la presidencia quien solicita el acuerdo de confidencialidad.

Gráfica 3: Documento acuerdo de confidencialidad, página 1

mc21 COLOMBIA

ACUERDO DE CONFIDENCIALIDAD

Parte reveladora: Mc21 Colombia SAS.

Responsable:

Parte receptora: Coordinación de Infraestructura.

Responsable:

Identificación del proyecto

Entre los firmantes identificados previamente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa a las siguientes consideraciones:

1. Que la información compartida en virtud del presente acuerdo pertenece a la **Mc21 Colombia SAS**, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto como quedo identificado anteriormente.

2. Que la información de propiedad de la empresa **Mc21 Colombia SAS** ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto y por otro lado la persona que dispone de la información para el presente caso actual como revelador, guarda y administrados de la información de propiedad de la empresa **Mc21 Colombia SAS.**

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente a la **Mc21 Colombia SAS,** así como también a no utilizar dicha información en beneficio propio ni de terceros.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

Fuente: El autor.

Imagen 4: Documento acuerdo de confidencialidad, página 2.

mc21
COLOMBIA

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, modelos de negocios y/o cualquier otra relacionada con el **proyecto** lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma la **Mc21 Colombia SAS,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

Fuente: El autor.

Figura 5: Documento acuerdo de confidencialidad, página 3.

mc21
COLOMBIA

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de la **Mc21 Colombia SAS.**

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Fuente: El autor.

Figura 6: Documento acuerdo de confidencialidad, página 4.

mc21
COLOMBIA

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

En Bogotá D.C., a los (21) días del mes de (Junio) de 2016

Como Parte Receptora: **Por la parte reveladora:**

Fuente: El autor.

¿Qué se va a hacer?

Se realizara una mejora a nivel de seguridad informática, lo cual se plantea en el presente proyecto como robustecimiento de seguridad red LAN corporativa, este de manera sistemática enfoca a nivel técnico cada uno de los ítems tecnológicos de la compañía y los asocia al modelo OSI.

El modelo OSI comprende 7 capas, pero se subdivide en 2 globales, capa de host orientada ésta a capa de aplicación y capa media, orientada ésta a infraestructura o backend.

Acorde a las dos capas previamente descritas se plantearán soluciones genéricas las cuales se encargaran de brindar de manera directa el aseguramiento a nivel de seguridad informática en los ítems que lo comprenden.

El proceso de robustecimiento se hará de la siguiente manera:

1. Capa de host:
    a. Actualización de parches a nivel de sistemas operativos.
        i. Configuración de WSUS, sistema encargado de enviar actualizaciones a los equipos del dominio.
        ii. Actualización de parches y aplicaciones en sistemas operativos LINUX.
    b. Actualización de licenciamientos de appliances, utm, firewalls y descarga de actualizaciones y fixes.
    c. Documentación y programación de actualizaciones.
    d. Instalación de consola de antivirus centralizada y configurada con gpo del dominio.
        i. Configurar encripción de disco duro bajo consola McAfee.
        ii. Configuración Data Protection McAfee para asegurar el inicio seguro de las estaciones de trabajo en el boot.
        iii. Configurar webmail control, este es un pluggin que se asocia al cliente Outlook, el cual permite escanear y monitorizar los emails que acceden y salen de las estaciones de trabajo.
        iv. Configurar en el OU del dominio, política de McAfee de Web Browser Control, que permite a nivel de capa de aplicación configurar políticas de acceso a sitios web detectando de manera proactiva y anticipada riesgos de malware, virus y posibles ataques por medio de accesos a internet desde estaciones de trabajo.

e. Instalación de Web Application Firewall (modsecurity), este elemento se instala en la capa de aplicación de los servidores web (webservices) que tienen sistema operativo Linux, este firewall posee triggers que permiten identificar las peticiones tipo http(s) y lograr identificar la fiabilidad de las peticiones descartando las que no son fiables, además de incorporar triggers tipo cross site scripring, entre otros.

2. Capa Media:
    a. Seguridad en networking, configurar en el firewall listas de control de acceso (ACL), en las mismas crear los grupos de usuarios que tendrán acceso a la red, esto a través de una configuración 802.1X asociado al AD.
        i. Actualización de FIXES, descarga de parches para UTM y Firewalls.
        ii. Habilitación de servicios y puertos desde el firewall permitiendo el consumo que es estrictamente necesario. Ejemplo: servicios FTP, SMTP, SSH, POP, IMAP, HTTP(S), entre otros.

¿Cómo se va a hacer?

Como primera instancia a como se realizará el proyecto de robustecimiento corporativo en la red LAN, se debe cuantificar la cantidad de ítems que van a ser manipulados, en otras palabras el inventario que existe. A continuación se describe la cantidad de equipos de cómputo, servidores y equipos de comunicación.

Tabla 1: Inventario de servidores.

SERVIDORES EN MC21 CALL 110				
ITEM	**NOMBRE DE SERVIDOR**	**IP**	**USUARIO**	**PUERTO**
1	FWBUILDER VIRTUALIZADO	192.168.0.251	root	22
2	PRUEBAS	192.168.0.108	root	22
3	CORREO_SIS	192.168.0.220	root	22
4	CORREO_MC21	192.168.0.221	Root	22
5	SERVER FILESERVER	192.168.0.4	RED / wropero	E R

6	serv-sarepoint	192.168.0.201	RED / wropero	E R
7	SERVER EXCHANGE// Active Directory	192.168.0.5	RED / wropero	E R
8	SERVERBI sin dominio	192.168.0.103	Administrador	E R
9	Serverbidev	192.168.0.126	Administrador//red	E R
10	Serberbi	192.168.0.120	Administrador//red	E R
11	Pharmtechdes	192.168.0.225	Root	22
12	Tableau	192.168.0.57	Administrador/wropero	E R
13	Desarrollo Oracle	192.168.0.142	Root	22
14	PLANTA TELF	192.168.0.246	Root	N/a

FISICOS
VIRTUALES
FISICOS

Fuente: El autor.

Tabla 2: Inventario de equipos PC.

NOMBRES Y APELLIDOS	NOMBRE PC	CPU			
		IP	SERIAL	MARCA	PROCESADOR
ING. GUILLERMO	INGINFRAEST-MC21	**192.168.0.85**	20QP3	HP	CORE 2 DUO
CRISTINA ROJAS	JEFCONT-MC21	**192.168.0.176**	200N5	HP	CORE 2 DUO
KATHERINE VARGAS	AUXCONT-MC21	**192.168.0.119**	200N4	HP	CORE 2 DUO
CAMILA RODRIGUEZ	CONTABIL1	**192.168.0.105**	00LQ	HP	CORE 2 DUO
MARTHA MONRROY	GESHUM-MC21	**192.168.0.121**	200K4	HP	CORE 2 DUO
ANGELICA MURILLO	ASISPRE1-MC21	**192.168.0.108**	1037J	HP	CORE 2 DUO
SONIA PARADA	COOROPEER-SIS	**192.168.0.72**	200NB	HP	CORE 2 DUO
JOHN OTERO	REPRESCLIENT-MC21	**192.169.0.87**	200MR	HP	CORE 2 DUO
PAOLA DUQUE	RECUPERADO	**192.168.0.99**	200P2	HP	CORE 2 DUO
SANDRA MATEUS	ANALISOPORT-SIS	**192.168.0.93**	200L6	HP	CORE 2 DUO
JEISSON PATIÑO	ANALISOPORT-SIS	**192.168.0.123**	200MD	HP	CORE 2 DUO
BRAYAN	REPRESERVI-SIS	**192.168.0.60**	200PD	HP	CORE 2 DUO

PERILLA					
CIRLEY URBINO	ANALISOPORT1-SIS	**192.169.0.125**	200N6	HP	CORE 2 DUO
MARCELA VASQUEZ	ANALISOPORT2-SIS	**192.168.0.91**	200Q6	HP	CORE 2 DUO
YESID TIBANA	ANALISOPORT4-SIS	**192.168.0.94**	200NZ	HP	CORE 2 DUO
LUIS MORENO	SOPORTE1	**192.168.0.77**	200NH	HP	CORE 2 DUO
DANIEL SALGADO	EQUIPO200Q7	**192.168.0.98**	ML-63194	HP	CORE 2 DUO
ANDRES VEGA	PRODESARR-SIS	**192.168.0.114**	ML-55576	HP	CORE 2 DUO
LILIANA MEDINA	PORDESARRO	**192.168.0.90**	ML-68071	HP	CORE I7
PATRICIA CANO	INGBI	**192.168.0.134**	ML-68117	HP	CORE I7
FELIPE HERNANDEZ	USUARIO2-PC	**192.168.0.117**	ML-59653	HP	CORE I7
LEONARDO SANCHEZ	DESA1MC21	**192.168.0.132**	ML-68116	HP	CORE I7
SANDRA GALLEGO	Eqipo200lv	**192.168.0.98**	200LV	HP	CORE 2 DUO
JOHN MOGOLLON	PRODESARRO	**192.168.0.113**	200LC	HP	CORE 2 DUO
IVONNE ALDANA	INGDESAR-SIS	**192.168.0.92**	200MP	HP	CORE 2 DUO
DIERICK DIAZ	USUARIO1-PC	**192.168.0.107**	ML-42685	HP	CORE I7
NIDIA GUTIERREZ	CLINICO5	**192.168.0.112**	ML-54812	HP	CORE 2 DUO
LAURA MALDONADO	CLINICO4	**192.168.0.102**	ML-32213	HP	CORE I7
DANIEL RIVERA//LIBRE	USUARIO2-PC	**192.168.0.215**	ML-43764	HP	CORE I7
SANDRA TORRES	CLINICO5	**192.168.0.123**	ML-43767	HP	CORE I7
WILLIAN HERNANDEZ	USUARIO4-PC	**192.168.0.130**	ML-38214	HP	CORE I7
CAMILO YATE	ESTADISTICO1	**192.168.0.139**	ML42677	HP	CORE I7
SALA JUNTAS	GERSERCLIN	**192.168.0.**	2RTM	HP	CORE 2 DUO
ALEJANDRO MURILLO-PORTATIL	GERTEC-MC21	**192.168.0.151**	N5KG	HP	CORE I5
LUIS ENRIQUE AYA-PORTATIL	GERCOMER-MC21	**192.168.0.100**	N5KH	HP	CORE I5
PIEDAD PINEDA	PRESIDENTE-MC21	**192.168.1.124**	DLP1	HP	CORE I5
ALVARO VALLEJOS-PORTATIL	GSERCLIN2	**192.168.0.187**	0HJP	HP	CORE I5
CAMILO BERNAL	GERPRODUCTOSIS	**192.168.0.157**	ML-62298	HP	CORE 2 DUO

Fuente: El autor.

Tabla 3: Inventario equipos de comunicación.

EQUIPOS DE COMUNICACIÓN	SWITCHES	SERIAL
SWITCH 1000 BASE X/T	3 COM 4500 PWR	A980
SWITCH 1000 BASE X/T	3 COM 4500 PWR	E480
SWITCH 1000 BASE X/T	HP V1910-24G	400G
PLANTA TELEFONICA	ALCATEL LUCENT	201
ROUTER	CISCO 2960 SERIE X	60B5
ADSL	HUAWEI ETB	H6530
APARATO FIBRA OPTICA	RAISECOM	RC512-FE-S
VoIP	vONAGE	186F
VoIP	VONAGE	46D
VoIP	CISCO GMS	90q2970

Fuente: El autor.

Posteriormente al inventario presentado previamente y acorde a la pregunta del **¿cómo se va a hacer?** Se plantea realizar dicha labor en un tiempo operativo de 14 semanas, más sin embargo la adquisición de licencias, compra y actualización de equipos de comunicaciones y de cómputo e incluyendo la planeación de este proyecto, presentación a la presidencia, autorización, investigación, ejecución y finalización dicho proyecto tendrá una duración de **52 semanas**.

Como primera instancia debe solicitarse a la presidencia el costo de la renovación de licenciamiento de appliances, en este caso firewalls, licencias de Linux (estas de Oracle Linux son anuales), licencias de antivirus, en este caso Mc Afee que es anual y licenciamiento de equipos que tienen Windows.

Esta es la base del proyecto, cumplir con los requisitos de licenciamiento de equipos tecnológicos para que posteriormente a esa base se empiecen las configuraciones basadas en buenas prácticas.

Para la programación del **¿cómo se va a hacer?** Se inserta la **tabla 4**, la cual comprende un **cronograma** netamente operativo contando con el licenciamiento y la inversión al 100% de la empresa, las cuales son labores administrativas que no serán contempladas en este proyecto, ya que este proyecto aún más que partir de bases investigativas es un proyecto netamente aplicado.

6. CRONOGRAMA

Tabla 4: Cronograma.

		Agosto				Septiembre				Octubre				Noviembre	
ACTIVIDAD PRINCIPAL	**ACTIVIDADES**	**semana 1**	**semana 2**	**semana 3**	**semana 4**	**semana 5**	**semana 6**	**semana 7**	**semana 8**	**semana 9**	**semana 10**	**semana 11**	**semana 12**	**semana 13**	**semana 14**
Actualización de Sistemas Operativos, Aplicaciones, RPM y Appliances.	Configuración WSUS en Windows Server.														
	Actualizar Servidores e instancias UNIX (Oracle Linux y RedHat Enterprise).														
	Actualización de Licenciamiento Appliances UTM (actuales)														
	Documentación de renovaciones y programación de seguimiento.														
Seguridad Networking.	Creación de ACL en la LAN para usuarios y servidores.														
	Políticas UTM por servicio														
	Instalación de Consola McAfee y asociación AD.														
Seguridad a nivel de capa de aplicación (7).	Encription Data														
	Data Protection														
	WebMail Control														
	Web Browser Control														
WAF	Instalación y configuración de 1 WAF centralizado el cual deberá cubrir las instancias WebServices de consumo.														
	Apuntamiento FQDN														
	Verificación de Amenazas WAF.														
	Re-Verificación de Amenazas WAF.														
Análisis de Vulnerabilidad.	Se realiza análisis de Vulnerabilidad caja blanca.														
	Evidencias de Hacking Ético.														
	Re-Afinación de WAF, UTM, Servidores, Instancias, etc... Dependiendo de Hacking Ético.														
	Control y Cierre														

Fuente: El autor.

¿Con qué se realizará?

Para la culminación de este proyecto, teniendo en cuenta el licenciamiento e inversión realizada al 100% los elementos utilizados son los siguientes:

1. Licenciamiento SONICWALL UTM tz500 (x1).
2. Licenciamiento Windows Server 2008R2 (x2).
3. Licenciamiento McAfee Consola Antivirus Orchestrator (x1).
4. Licenciamiento clientes EPO McAfee PC (x60).
5. WAF ModSecutiry, para versión Linux.
6. Herramienta Kali Linux.

Cuadro de costos:

Tabla 5: Cuadro de costos.

PRESUPUESTO			
Concepto	**Cantidad**	**Valor Unidad**	**Valor**
Actualización Licenciamiento Sonicwall TZ500	1	USD 1.500	USD 1.500
Licenciamiento Windows Server Open VL 2012 St Down	2	USD 1.200	USD 2.400
Consola EPO Orchestrator Mc Afee	1	USD 2.800	USD 2.800
Servicio de Configuración Consola McAffe + CLI	1	USD 350	USD 350
Clientes Mc Afee EPO	60	USD 13	USD 780
Licencias Oracle Enterprise Linux	2	USD 3.000	USD 6.000
	0	USD 0	USD 0
	0	USD 0	USD 0
	TOTAL	USD 8.863	USD 13.830

Fuente: El autor

7. REALIZAR ACORDE AL MODELO OSI, MEJORAS EN ROBUSTECIMIENTO DE LA RED LAN EN CADA UNA DE SUS CAPAS COMPRENDIDAS:

7.1 Actualización de Sistemas Operativos, Aplicaciones, RPM y Appliances:

Instalación y Configuración de servidor WSUS.

Entre las labores a nivel de seguridad que debe realizarse como buena práctica y a su vez de manera programada es la instalación de actualizaciones a los sistemas operativos, ya que muchas de las actualizaciones enviadas por los fabricantes corrigen fixes de seguridad, un ejemplo muy claro son las que envía Microsoft, quien periódicamente envía parches de actualización a los sistemas operativos que corrigen vulnerabilidades del mismo. Esto no solo en Windows, sino fabricantes como Oracle, envía periódicamente parches de actualizaciones a sus sistemas operativos, que optimizan el kernel y/o aplicaciones tipo MySQL entre otros.

Hay que tener en cuenta que en estas actualizaciones que deben realizarse de manera periódica pueden que haya algunas aplicadas a framework, java, apache y demás; esto obliga a ser muy cuidadoso debido que puede que ocurra algunos errores de ejecución de aplicaciones debido a versionamientos, y sea necesario realizar rollback en algunos casos puntuales.

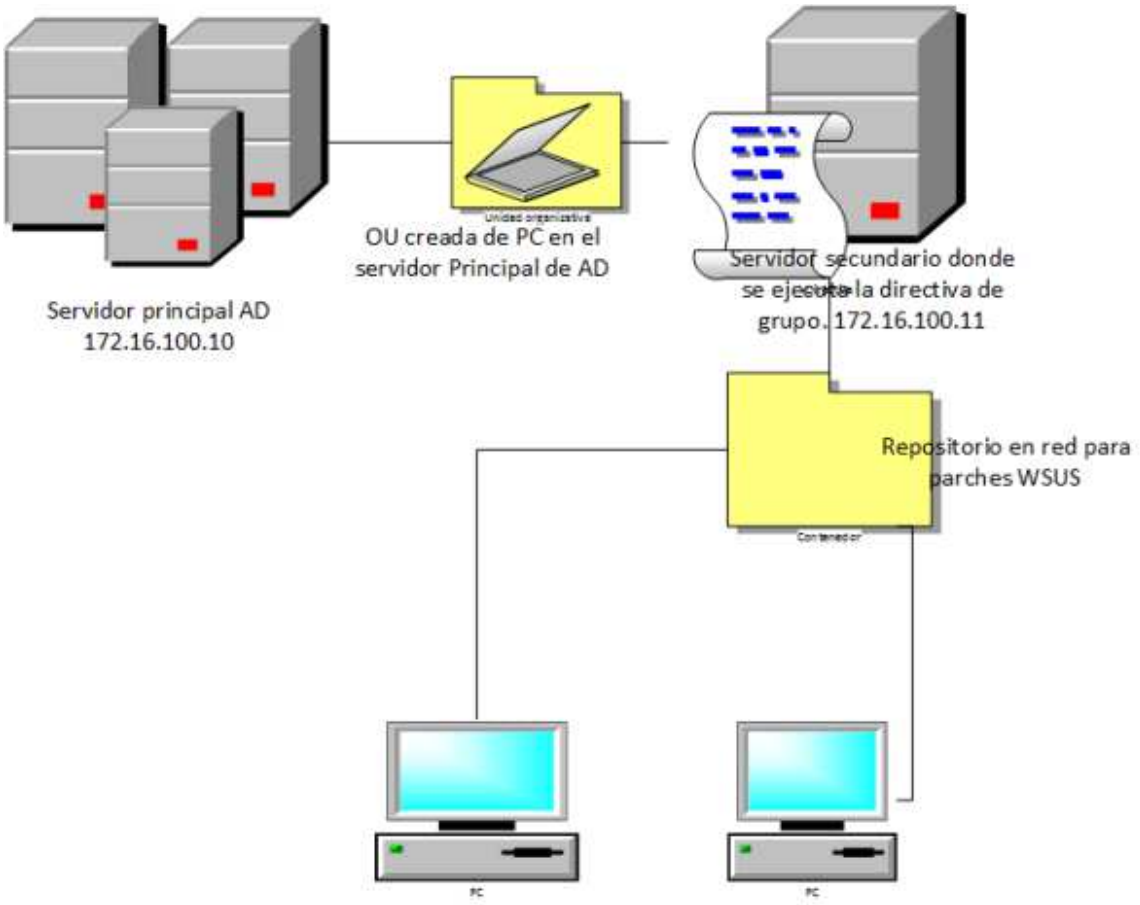
En este caso muy puntual en el cual se desarrolla este proyecto los sistemas operativos en la red LAN son Windows y Oracle LINUX, para los servidores Windows se implementa un WSUS el cual por GPO realiza cada 24 horas descarga de actualizaciones en los equipos cliente. En el caso de los Oracle Linux se realiza una programación para bajar por medio del YUM UPDATE cada 2 meses actualizaciones de los repositorios.

En la gráfica 2, se inicia la descripción de la configuración del WSUS, este refiere a Windows System Update Services, el cual se encargará de centralizar todas las actualizaciones de los equipos que estén registrados en el dominio, para cada una de las versiones de sistema operativo el mismo descargará las respectivas actualizaciones, en un repositorio en el disco duro, estas actualizaciones contemplan actualizaciones a aplicaciones del sistema operativo, actualizaciones

de seguridad, corrección de fixes y corrección a errores que puedan existir en las versiones de sistemas operativos registrados en el dominio.

Abajo se describe configuración en la LAN del WSUS:

Gráfica 2. Configuración lógica WSUS.

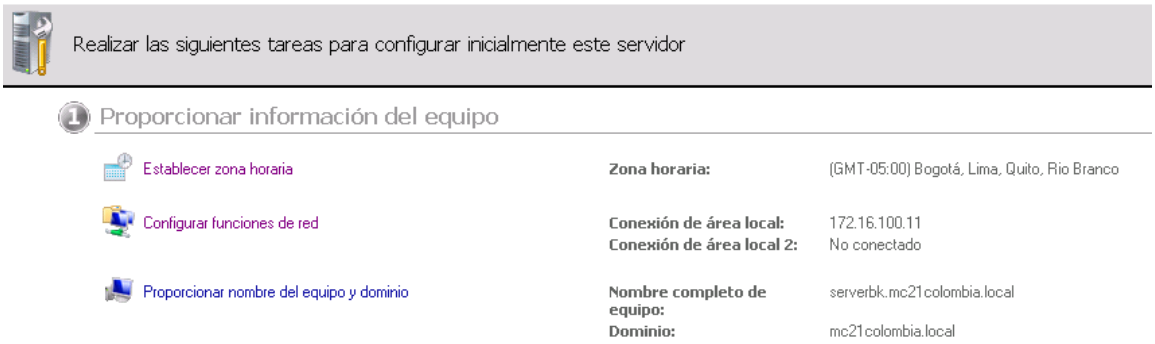


Fuente: El Autor.

Configuración Real de servidor 172.16.100.11.

La grafica previa describe la topología contemplada para el despliegue de un WSUS unificado a un domino de Windows corporativo, en el servidor 172.16.100.10 correspondiente a directorio activo se creará una Unidad Organizacional, en la cual se asocian los PC's del dominio y a su vez el servidor 172.16.100.11 correspondiente a WSUS se encargará de ejecutar una directiva de grupo en la cual las actualizaciones descargadas en el repositorio en red para parches de WSUS las cuales serán desplegadas a los equipos cliente.

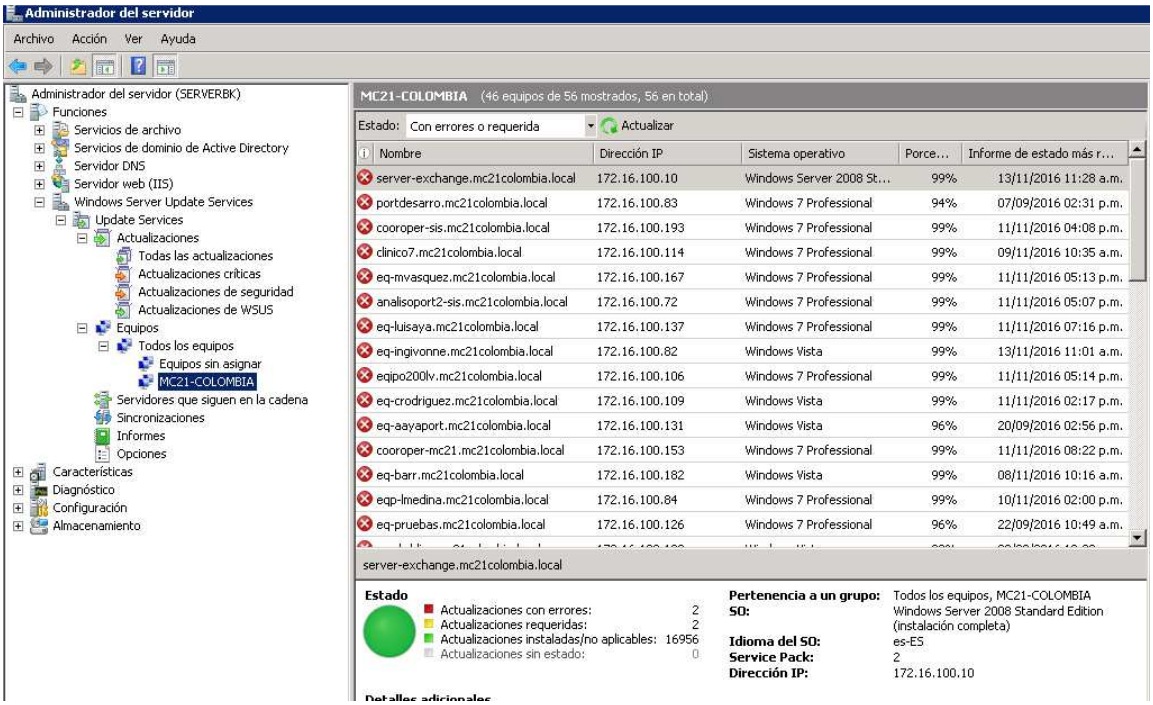
Gráfica 3. Servidor WSUS.



Fuente: El Autor.

La gráfica tres (3) denota una breve configuración del servidor, tal como lo es la IP, el dominio perteneciente y la zona horaria.

Gráfica 4: Árbol de WSUS.

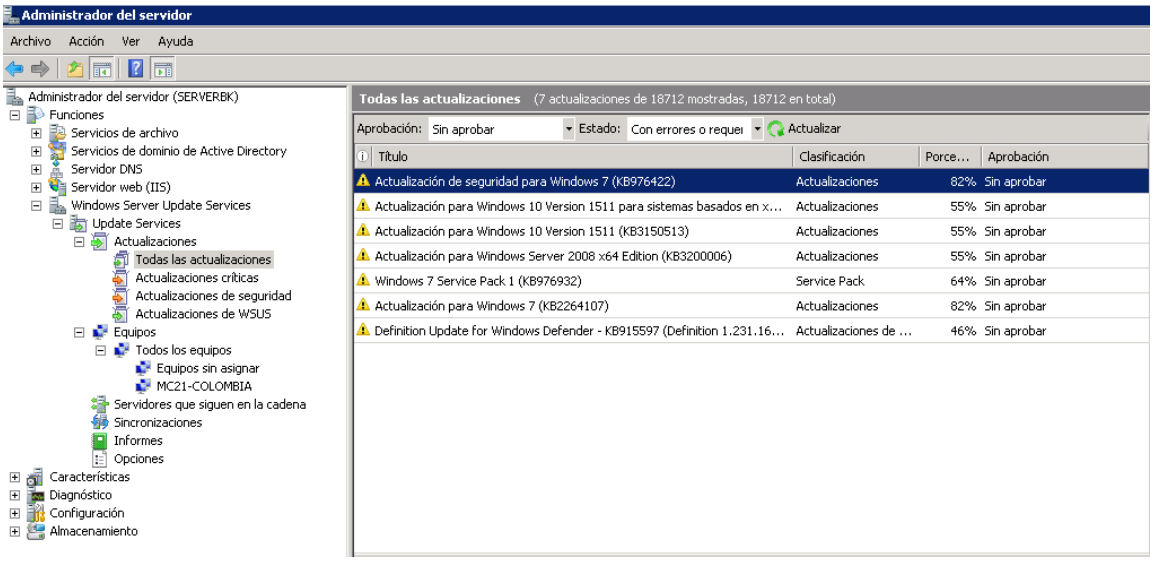


Fuente: El Autor.

La gráfica cuatro (4) permite divisar la OU (Unidad Organizacional) del WSUS en el cual se divisan los equipos que se encuentras suscritos al domino de MC21Colombia.local, en este caso. Los datos descritos en la OU corresponden al

nombre del equipo, dirección IP en la LAN, tipo de sistema operativo, porcentaje de actualizaciones y la fecha del último registro. Podríamos seleccionar algún equipo en especial y en la parte inferior de despliega una ventana la cual brindará una breve información del equipo y sus actualizaciones, así lograr determinar si está en riesgo o no debido a falta de actualizaciones.

Grafica 5: Resumen de actualizaciones Windows.

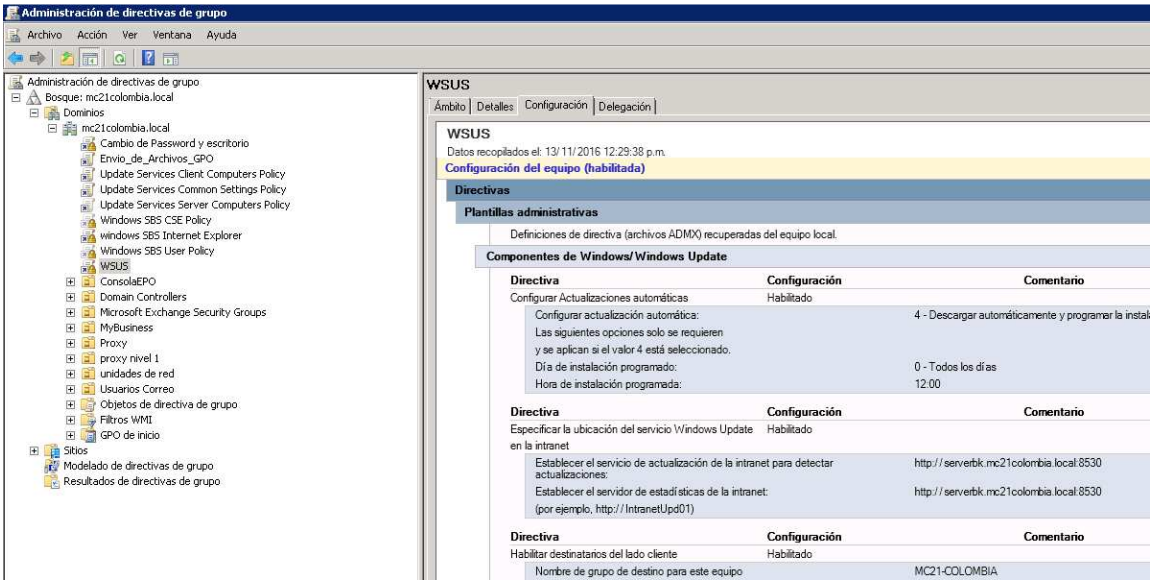


Fuente: El Autor.

La gráfica cinco (5) describe muy especialmente el tipo de actualizaciones que envía Microsoft al WSUS, entre las cuales se encuentran, actualizaciones críticas, actualizaciones de seguridad y actualizaciones WSUS. En este punto muy especial nos percatamos de lo importante que es tener un WSUS actualizado y funcionando en la organización debido a que sin este elemento en la red es muy complicado tener una política de seguridad en las estaciones de trabajo, esto enfocado a vulnerabilidades de software, bugs, fixes y demás de lo cual está muy por fuera del alcance de cualquier administrador de red u en vez muy dependiente de lo que el fabricante envié en lo que refiera a correcciones del mismo.

Lo recomendable es descargar todas y cada una de las actualizaciones de seguridad, debido a que existen hackers profesionales que logran detectarlas antes que el fabricante envíe las correcciones y ya con esta detección tempranera pueden llegar a atacar nuestros sistemas de información.

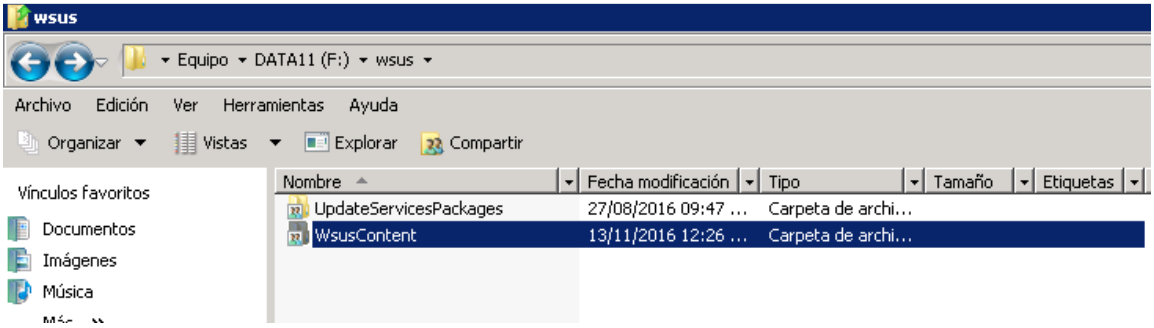
Grafica 6: GPO y programación de tarea.



Fuente: El Autor.

La gráfica seis (6) describe la manera correcta de cómo crear una política de grupo en la organización y a través de esta disparar las actualizaciones de manera programada y controlada desde la consola central a los equipos WSUS que se estén registrando en el dominio. Lo recomendable es configurarlas cada 24 hrs, ya que si tenemos actualizaciones constantes minimizaríamos el riesgo de infección por algún malware que ataque vulnerabilidades, errores, bugs entre otras fallas de Windows, las cuales son previamente corregidas.

Gráfica 7: Repositorio WSUS.



Fuente: El Autor.

En la gráfica siete (7) se muestra el path de actualizaciones en el WSUS, como buena práctica se recomienda dejarlo en una unidad independiente del sistema operativo, ya que pueden llegar a ocupar hasta 500GB de actualizaciones descargadas, y si lo tengo en un sistema en producción puedo dejar inoperante el mismo. En este caso se ha configurado el mismo y montado en un disco F:/DATA11/wsus.

El motivo de la implementación de WSUS en la red como robustecimiento de seguridad de la red LAN de MC21 Colombia es porque según Microsoft y sus [8]boletines de seguridad esta es la mejor manera de cubrir por medio de parches vulnerabilidades bajo Windows o virus que puedan llegar a afectar el sistema operativo.

Actualización de RPM servidores LINUX.

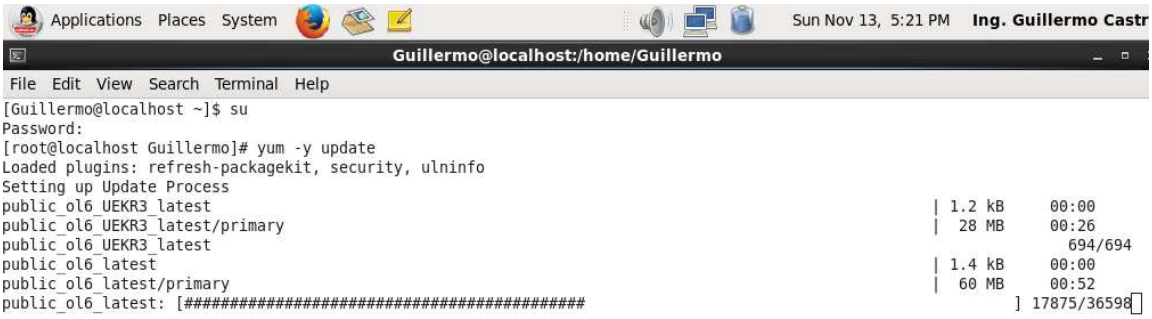
En el caso de los sistemas operativos basados en UNIX, las vulnerabilidades son menores ya que para ejecutar un software o aplicación es necesario estar con el root y compilar los RPM o binarios que lo conforman. Comúnmente los servidores de UNIX son utilizados para servicios de aplicaciones de consumo. En este caso MC21 Colombia los servidores UNIX cuentan con una arquitectura LAMP, lo cual traduce LINUX, APACHE, MYSQL y PHP. Las vulnerabilidades que se puedan encontrar en este tipo de arquitectura están más dadas a las mismas aplicaciones por lo tanto lo recomendable es estar en constante actualización de repositorios lo cual nos ayuda no solo a mejorar FIXES en las mismas sino vulnerabilidades que haya encontrado el fabricante en las mismas que puedan llegar a ser explotados por piratas informáticos.

Las actualizaciones en UNIX son más sencillas que en Windows, ya que para la arquitectura que se tiene solo basta con entrar a cada servidor y autenticarse como el root y efectuar un yum update sobre las aplicaciones o sobre el SO, pero antes de hacerlo hay que comprobar que no hayan incompatibilidad de los nuevos FIXES con la aplicación como Framework o demás que puedan llegar a entrar en conflicto, ya que una vez actualizados los mismos no hay vuelta atrás.

El Procedimiento de actualización es el siguiente por servidor:

[8] Boletines de seguridad de Windows, son artículos en los que Microsoft referencia los parches enviados y su funcionamiento para las diferentes versiones de Windows. La mayoría de estos buscan cubrir vulnerabilidades encontradas las cuales pueden ser explotadas por piratas informáticos. Véase en: https://technet.microsoft.com/es-es/security/bulletins.aspx

Grafica 8: Actualización servidores LAMP.



Fuente: El Autor.

Según el fabricante [9]Oracle Linux OS y su boletín se debe actualizar periódicamente los OS a medida que estos envíen notificaciones sobre los repositorios instalados, esto con el fin de minimizar vulnerabilidades y/o errores sobre las aplicaciones instaladas, por ejemplo APACHE 2.2.

Debido a la criticidad de estos servidores LAMP los cuales son el corazón del negocio no pueden estarse realizando constantes ventanas de mantenimiento para sus actualizaciones que pueden tardar largos periodo de tiempo y posterior a los mismos un reinicio requerido para que el Kernel se inicie con las nuevos parches descargados u optimizados, se decide programar una ventana de mantenimiento de Update cada 6 meses.

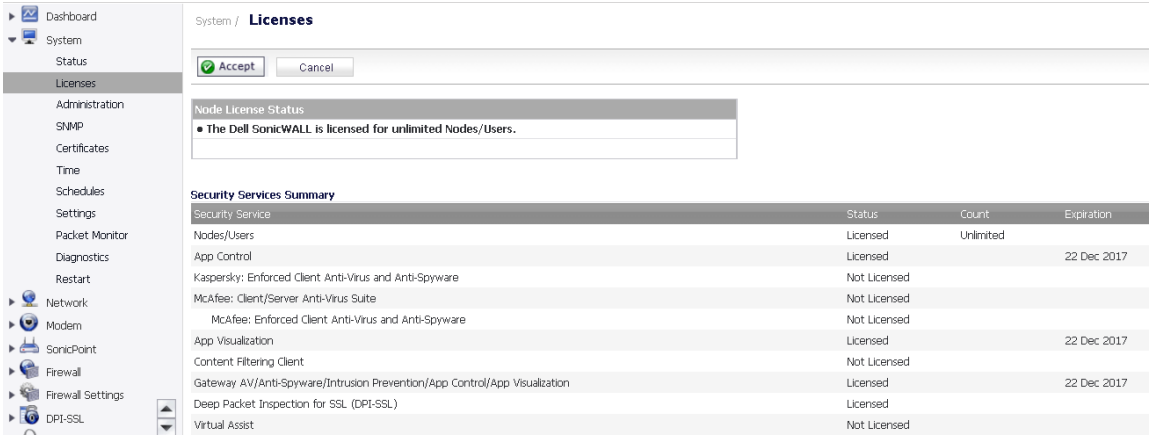
Licenciamiento UTM y Appliances:

Otro de los ítems importantes es tener el licenciamiento de los Appliances al día, en este caso el Firewall, debido a que el tenerlo actualizado permite que por parte de fabricante este envíe Fixes al firmware y actualizaciones de seguridad que

[9] Bulletin Oracle Linux OS, este reporta en su web oficial los fixes enviados de manera masiva a sus OS licenciados. véase en http://www.oracle.com/technetwork/topics/security/alerts-086861.html

previenen todo tipo de amenazas, como virus intrusiones, ataques de penetración y demás.

Gráfica 9: Licenciamiento al día de FW Sonicwall.



Fuente: El Autor.

Aunque hay que ser realista y el hecho de tener un Firewall actualizado y con las mejores configuraciones, no bastará para diferentes ataques de tipo botnet o tipo robot u otro tipo de amenazas inteligentes que se encuentran en la red. Pero aun así el licenciamiento no está de más.

TABLA 2: Programación para próximas actualizaciones.

Programación para próximas actualizaciones:

Última Actualización	**Efectuada por:**	**Sistemas Involucrados**	**Siguiente Actualización**
Septiembre 22 del 2017	Ing. Guillermo Castro	Clientes Windows Windows Server (Wsus) Appliance. Mc Afee	Diciembre 22 del 2017

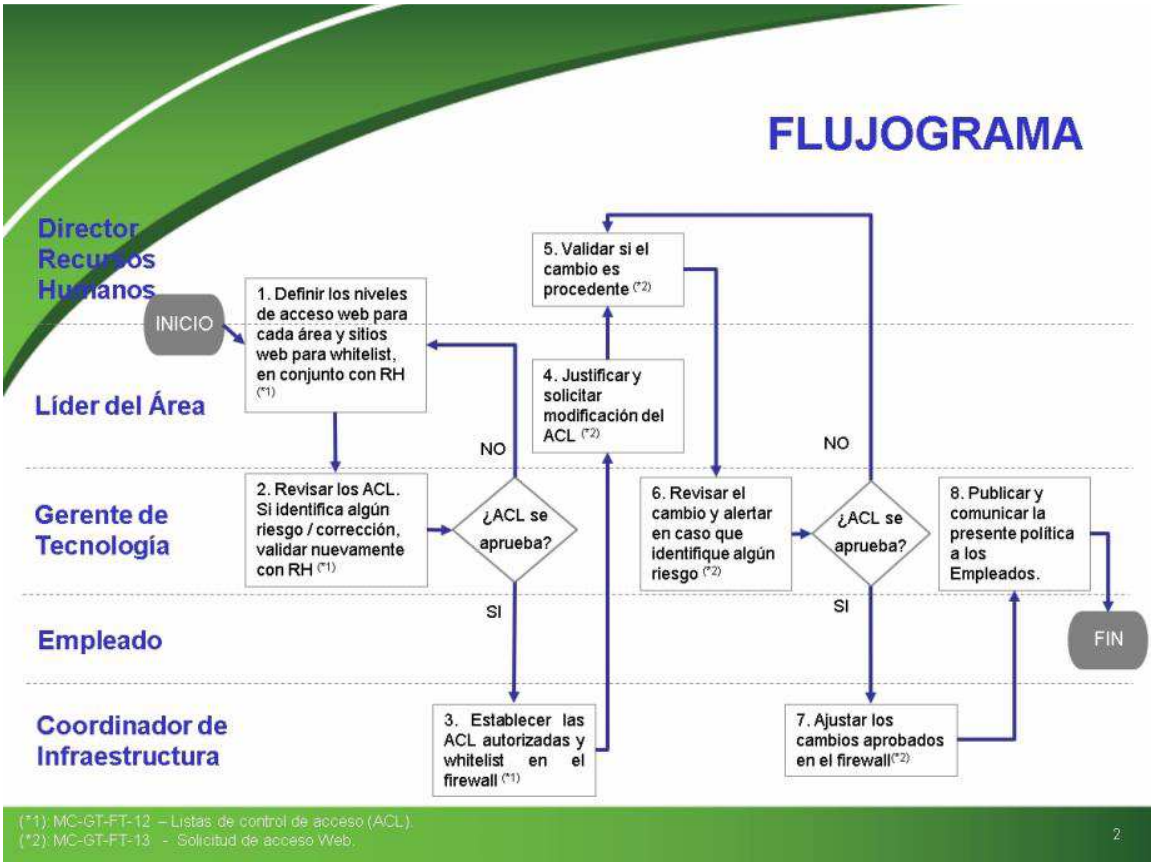
7.2 SEGURIDAD Y NETWORKING

Creación de ACL Para navegación:

Este ítem se divide en dos partes, la primera es la parte administrativa donde el director de RRHH establece con los líderes de cada área el contenido que debe tener habilitado los integrantes de sus respectivos grupos de trabajo. Acorde a estos se establecen ACL.

Abajo se describe el flujograma del proceso:

Gráfica 10: Flujograma de procesos MC21 Control Web.



Fuente: El Autor.

Se crea el formato de LISTAS DE CONTROL DE ACCESO y se publica, posteriormente se aplica en el UTM. Abajo se muestra el formato creado:

Tabla 3: Publicación de formato de ACL.

Nombre de lista de control de acceso	Categoría	Usuarios
ACL-ADMIN	Violence/Hate/Racism	Cristina Rojas
	Intimate Apparel/Swimsuit	Katherine Vargas
	Nudims	Camila Rodríguez
	Pornography	Jeffry Jojoa
	Weapons	
	Adult/Mature Content	
	Cult/Ocult	
	Drugs/ Illegal Drugs	
	Illegal Skills / Questionable Skills	
	Sex Education	
	Gambling	
	Ahcohol / Tobaco	
	Games	
	Hacking / Proxy Avoidance Systems	
	Humor / Jokes	
	Freeware / Software Downloads	
	Pay to Surf Sites	
	Kid Friendly	
	Advertisement	
	Web Hosting	
	Other	
	Social Networking	
	Malware	
	No Rated	
ACL-DEFAULT	Violence/Hate/Racism	Paola Duque
	Intimate Apparel/Swimsuit	Camilo Yate
	Nudims	Sandra Torres
	Pornography	Jorge Navarrete
	Weapons	Doc. Dieric
	Adult/Mature Content	William Hernandez
	Cult/Ocult	Daniel Villota
	Drugs/ Illegal Drugs	Ivan Erazo
	Illegal Skills / Questionable Skills	Sandra Mateus
	Sex Education	Andrés Navarrete
	Gambling	Sonia Parada
	Ahcohol / Tobaco	Marcela Vargas
	Games	Sandra Gallego
	Hacking / Proxy Avoidance Systems	Blanca Nidia Esperanza G.

	Humor / Jokes	Cirley Urbano
	Freeware / Software Downloads	
	Pay to Surf Sites	
	Kid Friendly	
	Advertisement	
	Social Networking	
	Malware	
	Job Search	
ACL-SERVERS	Violence/Hate/Racism	172.16.100.10
	Intimate Apparel/Swimsuit	172.16.100.11
	Nudims	172.16.100.12
	Pornography	172.16.100.13
	Weapons	172.16.100.14
	Adult/Mature Content	172.16.100.15
	Cult/Ocult	172.16.100.16
	Drugs/ Illegal Drugs	172.16.100.17
	Illegal Skills / Questionable Skills	
	Sex Education	
	Gambling	
	Ahcohol / Tobaco	
	Games	
	Hacking / Proxy Avoidance Systems	
	Humor / Jokes	
	Freeware / Software Downloads	
	Pay to Surf Sites	
	Kid Friendly	
	Advertisement	
	Social Networking	
	Malware	
	Job Search	
ACL-TECNOLOGIA	Violence/Hate/Racism	Ing. Guillermo Castro.
	Intimate Apparel/Swimsuit	Ing. Liliana Medina.
	Nudims	Ing. Ivonne Aldana.
	Pornography	Diego Barrios.
	Weapons	Richard Giraldo.
	Adult/Mature Content	Freddy Guerrero.
	Cult/Ocult	Jeison Patino.
	Drugs/ Illegal Drugs	Luis Eduardo.
	Illegal Skills / Questionable Skills	Sebastián Melo.
	Sex Education	
	Gambling	

	Ahcohol / Tobaco	
	Games	
	Hacking / Proxy Avoidance Systems	
	Humor / Jokes	
	Freeware / Software Downloads	
	Pay to Surf Sites	
	Kid Friendly	
	Advertisement	
	Social Networking	
	Malware	
	Job Search	
ACL-VIP	Violence / Hate / Racism.	Doc. Luis Enrique A.
	Intimate Apperal /Swimsuit	Doc. Alvaro V.
	Nudism	Ing. Guillermo G.
	Pornography	Ing. Domingo A.
	Weapons	Doc. Marileny Lugo.
	Adult / Mature Content	Angelica Murillo
	Cult / Ocult	Angela Aya
	Dugs / Illegal Drugs	
	Illegal Skill / Questionable Skills	
	Sex Education	
	Gambling	
	Hacking / Proxy Avoidance	
	Malware	

Fuente: El Autor.

Posterior a la publicación se realiza la configuración y puesta en marcha de las ACL en el FW.

Gráfico 11: ACL en UTM Sonicwall.

Application Objects

#	Name	Object Type	Match Type	Object Content
1	ACL-ADMIN	CFS Category List	N/A	1: Violence/Hate/Racism 2: Intimate Apparel/Swimsuit 3: Nudism 4: Pornography 5: Weapons 6: Adult/Mature Content 7: Cult/Occult 8: Drugs/Illegal Drugs 9: Illegal Skills/Questionable Skills 10: Sex Education ...
2	ACL-DEFAULT	CFS Category List	N/A	1: Violence/Hate/Racism 2: Intimate Apparel/Swimsuit 3: Nudism 4: Pornography 5: Weapons 6: Adult/Mature Content 7: Cult/Occult 9: Illegal Skills/Questionable Skills 10: Sex Education 11: Gambling ...
3	ACL-SERVERS	CFS Category List	N/A	1: Violence/Hate/Racism 2: Intimate Apparel/Swimsuit 3: Nudism 4: Pornography 5: Weapons 6: Adult/Mature Content 7: Cult/Occult 8: Drugs/Illegal Drugs 9: Illegal Skills/Questionable Skills 22: Games ...
4	ACL-TECNOLOGIA	CFS Category List	N/A	1: Violence/Hate/Racism 2: Intimate Apparel/Swimsuit 3: Nudism 4: Pornography 5: Weapons 6: Adult/Mature Content 7: Cult/Occult 8: Drugs/Illegal Drugs 9: Illegal Skills/Questionable Skills 10: Sex Education ...
5	ACL-VIP	CFS Category List	N/A	1: Violence/Hate/Racism 2: Intimate Apparel/Swimsuit 3: Nudism 4: Pornography 5: Weapons 6: Adult/Mature Content 7: Cult/Occult 9: Illegal Skills/Questionable Skills 10: Sex Education 11: Gambling ...

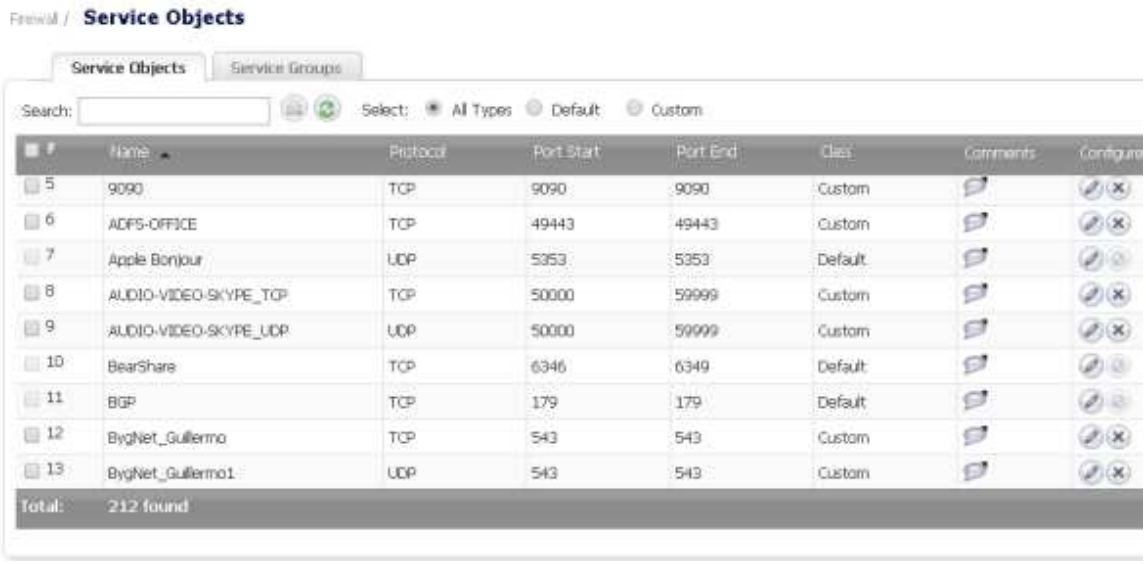
Fuente: El autor.

Políticas en UTM por servicio:

Una parte muy importante de la seguridad de lo que entra y sale de la LAN corporativa son los servicios, traducidos en puertos; en el cual la política es solo habilitar los puertos de servicios que se deben utilizar necesariamente. Los que no se utilizan se deniegan.

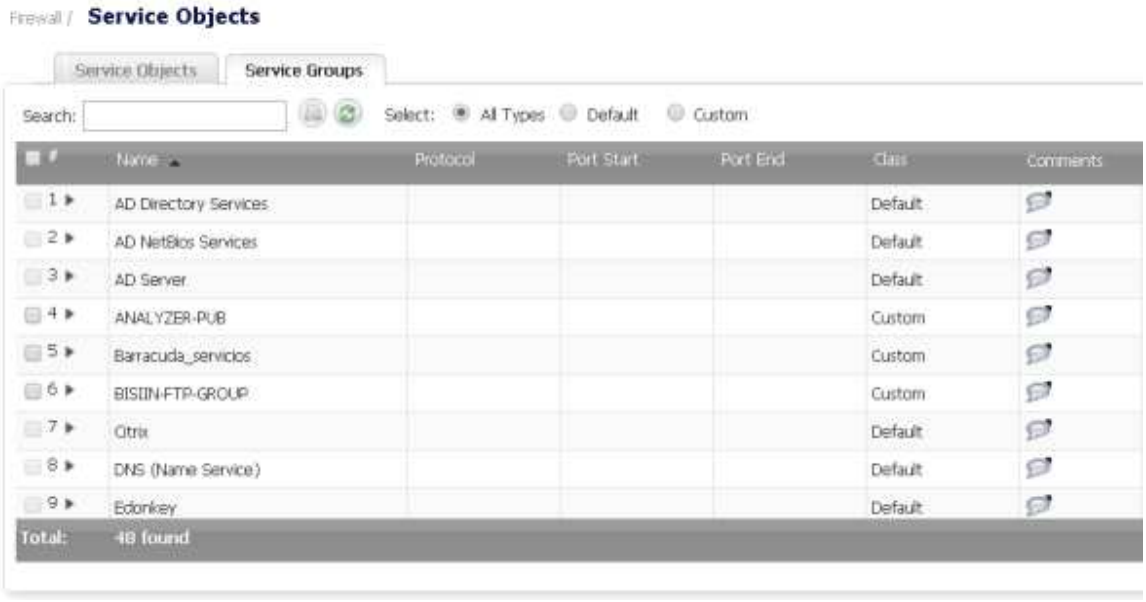
La configuración se hace de dos maneras, la inicial por Objetos en la cual se personalizan los puertos, ejemplo: 5060 por UDP para VoIP. Y la segunda manera es por Grupo de servicios, ejemplo: Resolución DNS.

Gráfico 12: Objetos por Servicios FW.



Fuente: El autor.

Gráfica 13: Servicios por grupos.



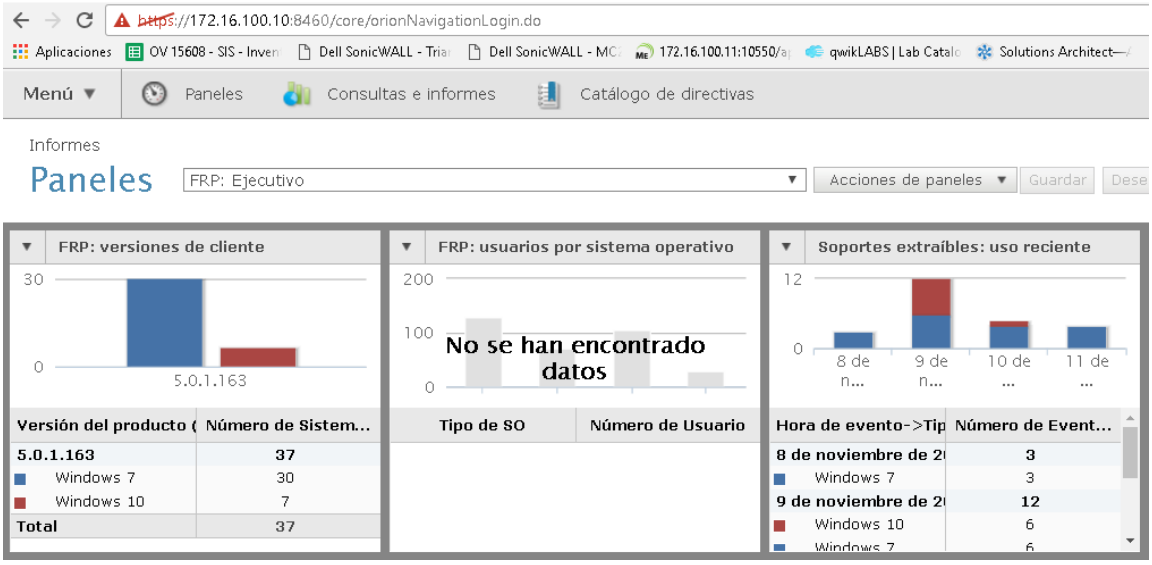
Fuente: El autor.

Instalación de Mc Afee Antivirus e integración con AD:

El hecho de instalar un antivirus configurado centralizado en un servidor de AD es el tener el control de los EndPoints a nivel de capa 7 (si se habla a nivel del modelo OSI), o bien llamada capa de aplicación. Se tiene entendido que la configuración de Firewall y UTM actúan a mayor medida en capa 3/4 lo cual es muy fácil de vulnerar con herramientas de Hacking y/o Botnets. El hecho de actuar a nivel de capa 7 permite tener un control por software de los dispositivos creando ACL entre ellos.

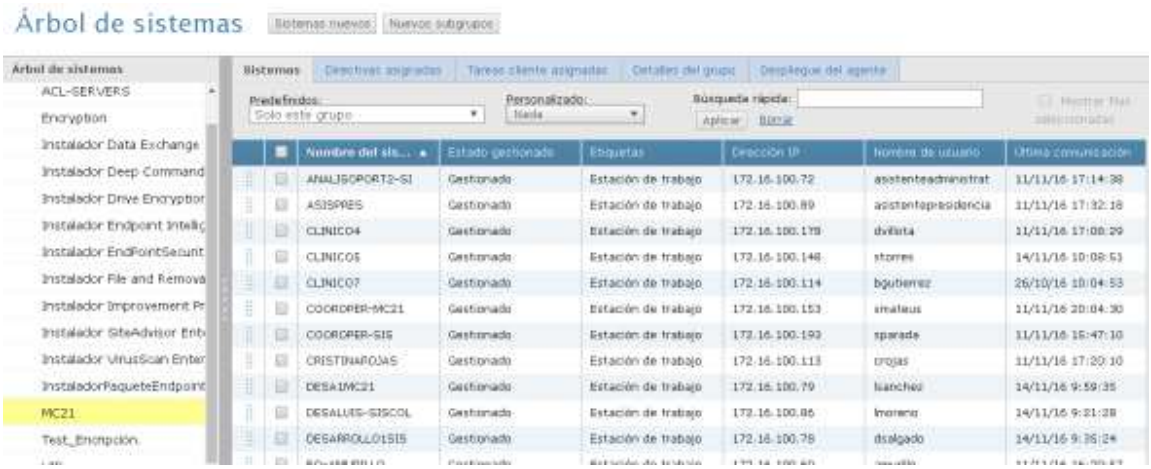
Se realiza la instalación de la consola Mc Afee Orchestator en el servidor principal de dominio en el cual se configura la política en el que por PC en el dominio se envían las directivas de seguridad. Así como los complementos de los Deploy.

Gráfica 14: Instalación Mc Afee en AD principal.



Fuente: El Autor.

Gráfica 15: Directiva por PC en el AD.



Fuente: El Autor.

Como política de seguridad se programa que cada semana se ejecuten análisis bajo demanda de los equipos ingresados en la consola de Mc Afee. De tal manera siempre este tendrá al día las librerías de Mc Afee que bajan de la nube del fabricante.

Grafica 16: Directiva de Scan On Demand.

Fuente: El autor.

Posteriormente a la configuración de los scan de los equipos por GPO, se realiza la configuración de seguridad de los agentes y sus paquetes de firewall sobre los endpoints en la LAN. Así como la actualización de librerías de virus.

Gráfica 17: Parametrización de configuración EndPoints.

Fuente: El Autor.

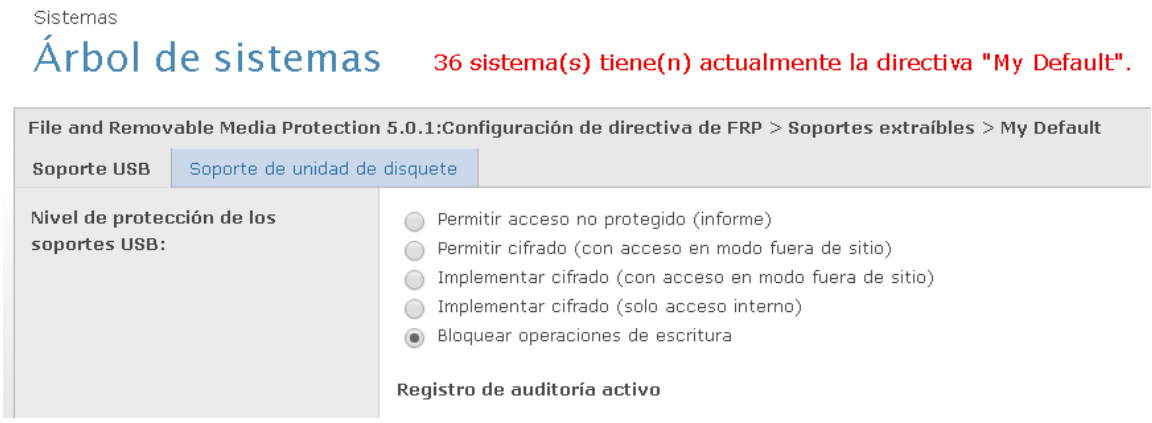
Una vez ya terminado toda la parte de los EndPoints a nivel de seguridad se procede a crear las directivas de control de extracción de información de los EndPoints, siendo está catalogada como posible fuga de información de los usuarios internos quienes pueden legar a hurtar la información y venderla.

Se crea la ACL en la cual se configurará la directiva File and Removable Media Protection, la cual solo permite acceso de lectura a los EndPoints dentro de esta ACL, más no de escritura imposibilitando la salida de información.

Grafica 18: Directiva File and removable Media Protection.

Fuente: El Autor.

Grafica 19: Directiva de Bloqueo de operaciones de escritura.

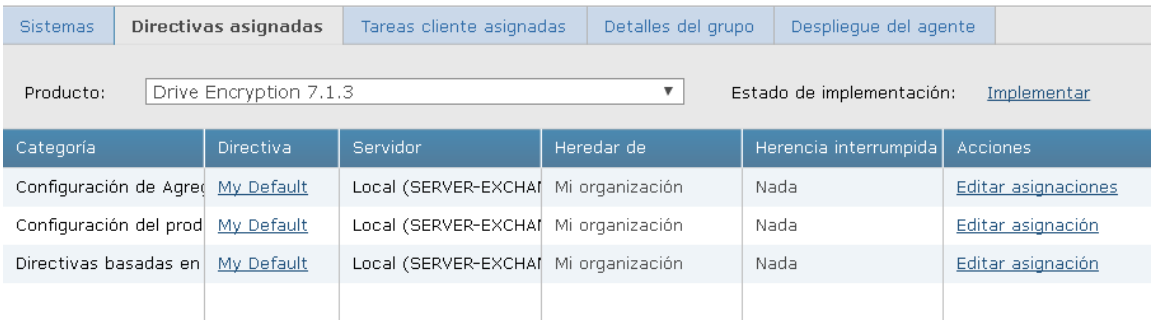


Fuente: El Autor.

Para finalizar con el Mc Afee, otra directiva muy importante es la Encripción de disco, la cual por medio del agente de Mc Afee desde el inicio del boot del equipo genera una autenticación con el AD del usuario que lo está utilizando. Si no se ingresa esta password correspondiente el sistema operativo no sube.

Si el equipo es hurtado y desea accederse a la información que contiene el mismo, este tendrá un algoritmo de cifrado de tipo militar el cual no permitirá reconocer la información que lo contiene.

Grafica 20: Directiva Drive Encryption Mc Afee.



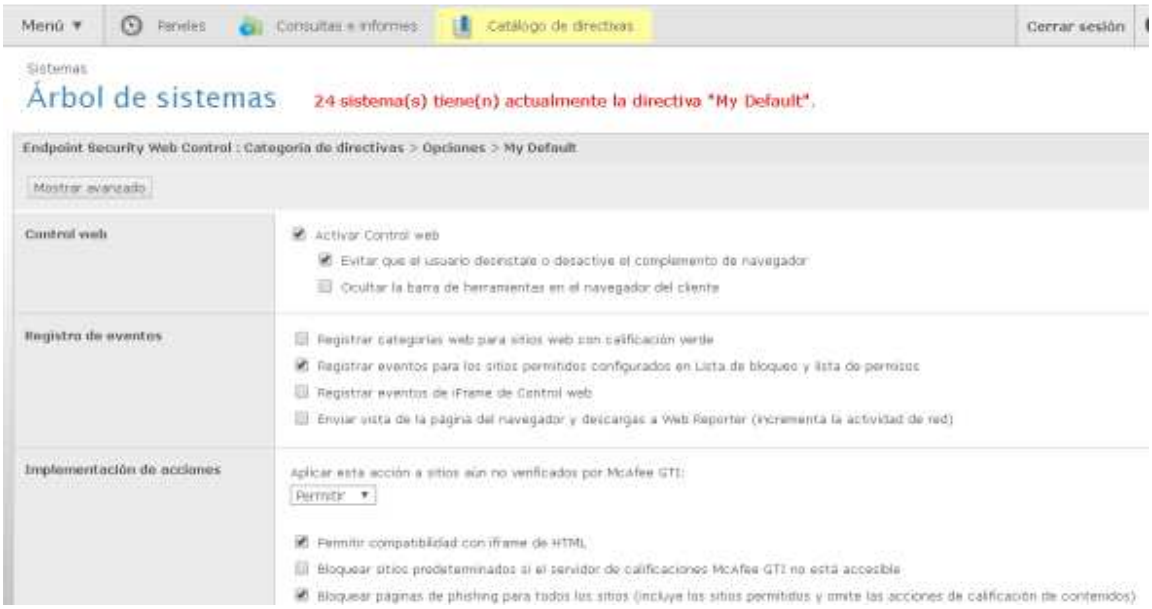
Fuente: El autor.

Gráfica 21: Directiva Drive Encryption Mc Afee Disk.

Fuente: El autor.

A nivel de conectividad y evitando descarga del Malware y/o acceso a contenido no permitido por la organización se efectúa la configuración de control e contenido WEB para los equipos en la LAN, el cual previene de todo tipo de ataques inteligentes y ejecuciones de tipo robot.

Gráfica 22: Configuración WebControl.



Fuente: El Autor.

Referente a la capa de aplicación de los EndPoints se configura el plugin para el cliente de correo electrónico, el cual en este caso es un Exchange. Este plugin se encarga de realizar un escáner previo de cada mensaje enviado por correo electrónico antes de que el usuario final tenga acceso a la bandeja, realizando de manera proactiva la validación de los correos evitando que de manera directa o indirecta un malware pueda llegar a ser no solo descargado sino ejecutado en el equipo cliente.

Esta es una manera muy común de recibir ataques por este medio, la técnica más utilizada es el phishing, en el cual se envía un correo tratando de engañar al usuario final con la intensión que este realice la descarga del archivo.

En la configuración actual en el robustecimiento de la red LAN corporativa se realiza la instalación del cliente McAfee de una Consola EPO Orchestrator, el cual realizará despliegues del plugin del Exchange tal como lo muestra la figura 24.

Gráfica 23: Configuración Seguridad de Exchange.

Fuente: El Autor.

7.3 INSTALACIÓN WAF (Web Application Firewall)

Como último ítem en el proceso de robustecimiento de una red LAN corporativa se realiza la instalación de un Web Application Firewall, este refiere a un firewall inteligente el cual logra detectar ataques de malware, ataques de denegación de servicio (DoS), Cross Site Scripting, SQL Injection y demás tipos de ataques que busquen vulnerar servicios que son consumibles y/o publicados hacia internet.

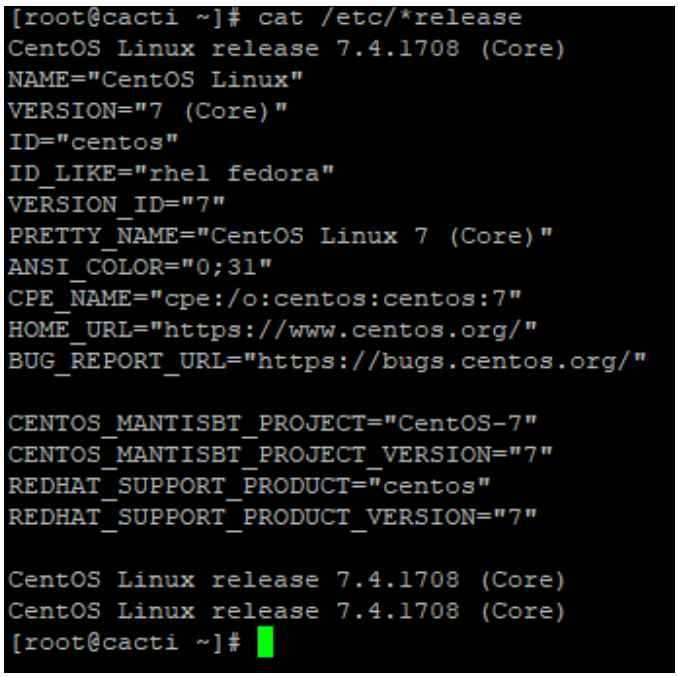
En este caso se va a instalar y a realizar la respectiva configuración de un WAF en Centos 7.0 llamado ModSecutiry el cual será integrado a un Apache de un WebService.

La configuración es la siguiente:

Sobre una instalación en un webservice (apache) se realiza la validación del SO, tipo y versión; en este caso es un Centos 7.4 Core, posterior a la validación del mismo se debe buscar el paquete que de WAF sea compatible.

Un comando que nos ayuda a verificar paquetes y compatibilidad del sistema operativo actual es el yum seach “nombre de paquete”; en este caso el comando será **yum search mod_secutiry.**

Gráfica 24: Validación de Sistema Operativo Centos.

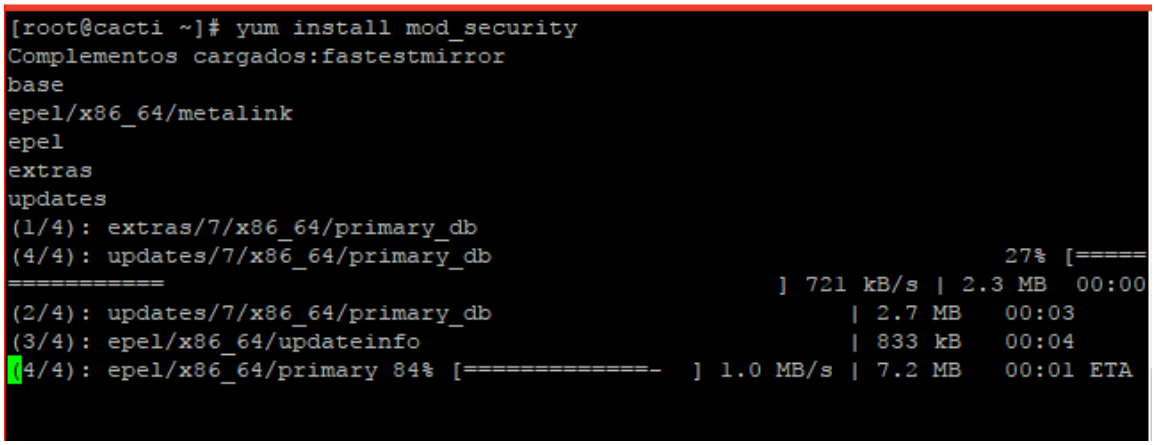


Fuente: El autor.

Después de haber ubicado y/o identificado el paquete a instalar del Mod_Secutiry se procede con el gestor de descargas YUM a realizar la instalación del Mod_Secutiry, el cual cumplirá la función de firewall inteligente a nivel de capa de aplicación en el webservice.

A continuación se muestra la instalación del mismo en el Centos referenciado previamente:

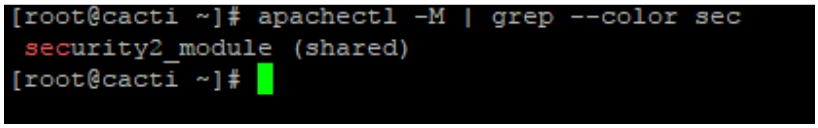
Gráfica 25: Instalación WAF.



Fuente: El autor.

Posterior a su instalación se valida con el comando GREP que el Mod_Secutiry se halla integrado al Apache como un módulo de seguridad de la siguiente manera:

Gráfica 26: Validación de integración WAF a Apache.



Fuente: El autor.

Después de su validación de integración al Apache, se revisa en el archivo mod_secutity.conf en el cual se habilitan las opciones SecRuleEngine y SecrequestBodyAccess, las dos en ON.

Estos dos módulos dependiendo de su estado ON u OFF permiten el activar y desactivar respectivamente las reglas de identificación de malwares y/o ataques, esto a través de triggers integrados en la aplicación.

En resumen estas dos opciones sirven para habilitar los otros módulos de seguridad del Apache.

A continuación se muestra el archivo de configuración descrito previamente en el WAF.

Gráfica 27: Verificación archivo de configuración WAF.

```
[root@cacti /]# cat /etc/httpd/conf.d/mod_security.conf
<IfModule mod_security2.c>
    # ModSecurity Core Rules Set configuration
        IncludeOptional modsecurity.d/*.conf
        IncludeOptional modsecurity.d/activated_rules/*.conf

    # Default recommended configuration
    SecRuleEngine On
    SecRequestBodyAccess On
    SecRule REQUEST_HEADERS:Content-Type "text/xml" \
         "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"
    SecRequestBodyLimit 13107200
    SecRequestBodyNoFilesLimit 131072
    SecRequestBodyInMemoryLimit 131072
    SecRequestBodyLimitAction Reject
    SecRule REQBODY_ERROR "!@eq 0" \
    "id:'200001', phase:2,t:none,log,deny,status:400,msg:'Failed to parse request body.',logdata:'%{reqbody_error_msg}',severity:2"
    SecRule MULTIPART_STRICT_ERROR "!@eq 0" \
    "id:'200002',phase:2,t:none,log,deny,status:44,msg:'Multipart request body \
    failed strict validation: \
    PE %{REQBODY_PROCESSOR_ERROR}, \
    BQ %{MULTIPART_BOUNDARY_QUOTED}, \
    BW %{MULTIPART_BOUNDARY_WHITESPACE}, \
    DB %{MULTIPART_DATA_BEFORE}, \
    DA %{MULTIPART_DATA_AFTER}, \
    HF %{MULTIPART_HEADER_FOLDING}, \
    LF %{MULTIPART_LF_LINE}, \
    SM %{MULTIPART_MISSING_SEMICOLON}, \
    IQ %{MULTIPART_INVALID_QUOTING}, \
    IP %{MULTIPART_INVALID_PART}, \
    IH %{MULTIPART_INVALID_HEADER_FOLDING}, \
    FL %{MULTIPART_FILE_LIMIT_EXCEEDED}'"
```

Fuente: El autor.

La gráfica 29 describe los cambios que deben realizarse para prender y/o activar las opciones de seguridad en el apache con el Mod_Secutiry a nivel de capa de aplicación (O capa de host según el modelo OSI).

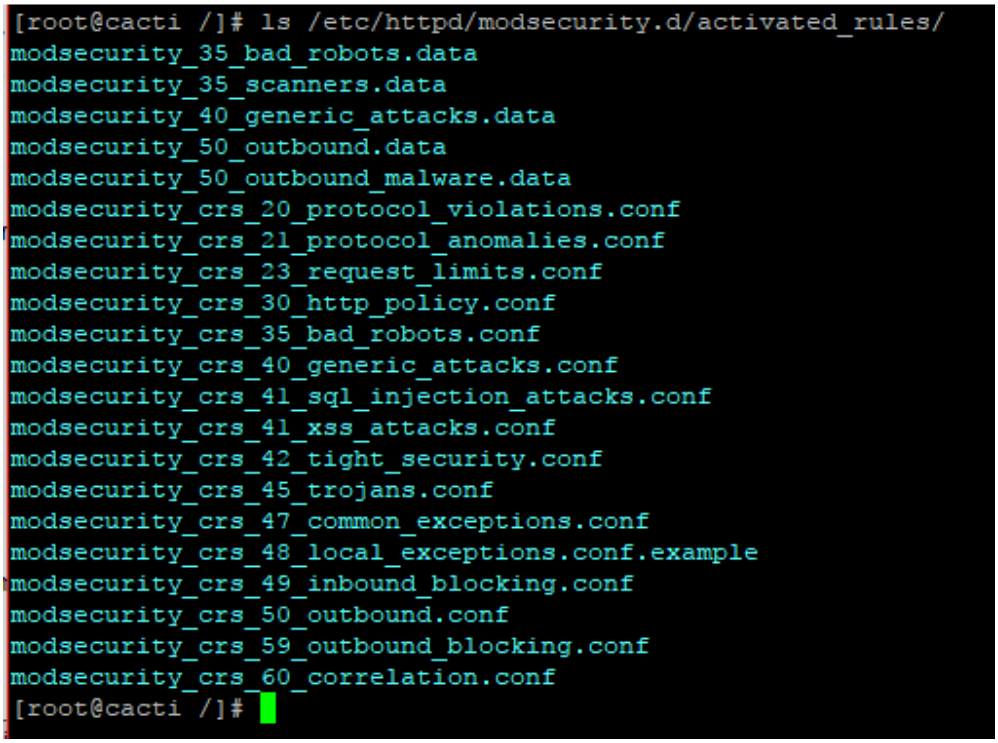
Gráfica 28: Prender opciones de reglaje.

```
<IfModule mod_security2.c>
    # ModSecurity Core Rules Set configuration
        IncludeOptional modsecurity.d/*.conf
        IncludeOptional modsecurity.d/activated_rules/*.conf

    # Default recommended configuration
    SecRuleEngine On
    SecRequestBodyAccess On
    SecRule REQUEST_HEADERS:Content-Type "text/xml" \
         "id:'200000',phase:1,t:none,t:lowercase,pass,nolog,ctl:requestBodyProcessor=XML"
    SecRequestBodyLimit 13107200
    SecRequestBodyNoFilesLimit 131072
    SecRequestBodyInMemoryLimit 131072
    SecRequestBodyLimitAction Reject
    SecRule REQBODY_ERROR "!@eq 0" \
```

Fuente: El autor.

Una vez después de prendido las opciones de seguridad se proceden a validar el repositorio de configuración de los triggers que componen las verificaciones contra ataques al WebService, Esto en la siguiente ruta:

Gráfica 29: Validación de triggers antimalware.



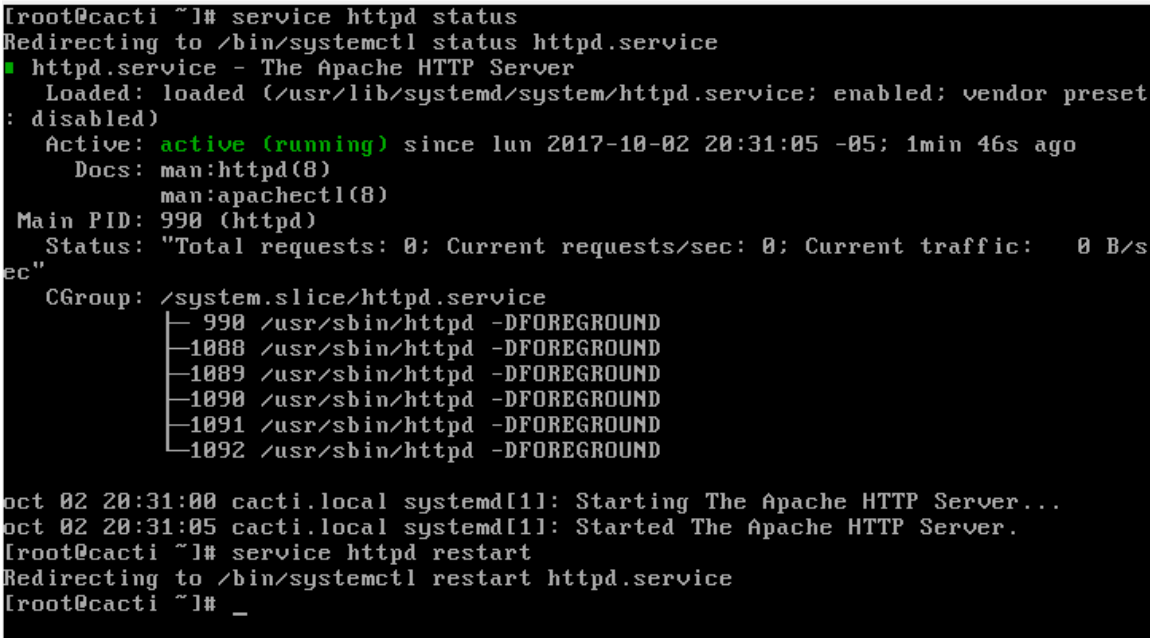
Fuente: El autor.

Los triggers mostrados previamente en el repositorio referenciado permiten de manera inteligente contener ataques ya sean tipo robot, de escáner, ataques genéricos, malwares, violaciones de protocolos, protocolos anómalos, ataques de tipo robot, sql Injection, xss ataques, trojanos, entre otros tipos de ataques.

Y así se finaliza la instalación del WAF en un apache, como último paso se debe reiniciar el apache para guardar los cambios e integración. Dicho reinicio se puede hacer con el comando **service httpd restart** o **/etc/iniy.d/httpd restart** cualquiera de los dos nos funciona de manera correcta.

A continuación se muestra el proceso de reinicio del apache en la gráfica 31:

Gráfica 30: Reinicio servicio Apache.



Fuente: El autor.

8. REALIZAR PROCESO DE ANÁLISIS DE VULNERABILIDADES SOBRE LA INFRAESTRUCTURA CONFIGURADA.

El análisis de vulnerabilidad consta de realizar unas pruebas de manera sistemática intentando acceder a la red y/o vulnerar la misma para lo cual se utilizaran diferentes herramientas acorde al orden planteado en el Modelo OSI, iniciando desde la capa uno (1) física hasta llegar a capa siete (7) aplicación.

Como se había referenciado previamente se ha subdividido el modelo OSI en dos capas macro, la primera llamada capa de media y la segunda llamada capa de host.

La primera capa referencia lo que compete a Netwoking y para lograr vulnerar la misma se utilizaran herramientas de hacking para escanear la red, lograr detectar vulnerabilidades, puertos, errores de configuración y comenzar a realizar ataques de DoS.

Dependiendo de lo que se evidencia se debe proceder con la capa de host. Hay que tener en cuenta que si no se logra vulnerar la primera capa, no se podrá llegar a la segunda, ya que a nivel de ingeniería como lo enuncia el modelo OSI no se puede llegar a la capa de aplicación sin antes haber pasado las seis capas previas.

El primer análisis de vulnerabilidad se realizará con una herramienta llamada Nmap, el cual realizará un escaneo minucioso identificando por donde se puede acceder a la red y vulnerarla.

A continuación las diferentes maneras de realizar el escaneo:

Nmap –V: Este refiere a hacer un escaneo verbose. Escanea todos los 65538 puertos vía TCP y UDP.

Nmap –sA: Este sirve para identificar si existe algún firewall en medio.

Nmap –A: Mapear todo (all); esta opción permite identificar sistema operativo, puertos y protocolos en uso y dependiendo de la configuración de la red hasta firewalls y switches.

La gráfica 32 demuestra el primer mapeo de puertos vía TCP y UDP.

Gráfica 31: Mapeo del host con puertos:

```
root@curso:/# nmap -v 192.168.0.22

Starting Nmap 6.00 ( http://nmap.org ) at 2017-10-03 00:32 ART
Initiating ARP Ping Scan at 00:32
Scanning 192.168.0.22 [1 port]
Completed ARP Ping Scan at 00:32, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:32
Completed Parallel DNS resolution of 1 host. at 00:32, 0.29s elapsed
Initiating SYN Stealth Scan at 00:32
Scanning 192.168.0.22 [1000 ports]
Discovered open port 80/tcp on 192.168.0.22
Discovered open port 22/tcp on 192.168.0.22
Completed SYN Stealth Scan at 00:32, 6.07s elapsed (1000 total ports)
Nmap scan report for 192.168.0.22
Host is up (0.0017s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
587/tcp closed submission
MAC Address: 08:00:27:2B:44:DA (Cadmus Computer Systems)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
           Raw packets sent: 1990 (87.544KB) | Rcvd: 15 (948B)
```

Fuente: El autor.

Se evidencia que solo se tiene abierto el puerto 22 y el 80, este último haciendo referencia al http. El puerto 22 nativamente es el puerto del SSH, una de las buenas practicas que se debe utilizar al tener un WebService publicado a internet, es cambiar dicho puerto SSH por otro ya que un ataque de tipo robot podrá realizar intento de autenticación con el root al puerto 22 y será cuestión de tiempo lograr acceder al servidor.

Otra buen práctica aparte de cambiar el puerto 22 del protocolo SSH es el editar el archivo de configuración del mismo, y bloqueando la opción del login con root vía SSH.

Proseguimos con los escaneos a nivel de networking y después hacemos los ajustes correspondientes.

Gráfica 32: Mapeo a host intentando determinar firewall activo.

```
root@curso:/# nmap -sA 192.168.0.22

Starting Nmap 6.00 ( http://nmap.org ) at 2017-10-03 00:34 ART
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.47 seconds
root@curso:/# nmap -PN 192.168.0.22

Starting Nmap 6.00 ( http://nmap.org ) at 2017-10-03 00:35 ART
Nmap scan report for 192.168.0.22
Host is up (0.0017s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
587/tcp closed submission
MAC Address: 08:00:27:2B:44:DA (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 7.31 seconds
root@curso:/#
```

Fuente: El autor.

La grafica 33 realiza un mapeo total al servidor, el cual logra identificar el sistema operativo, el tipo de kernel en este caso 2.6 y el equipo de comunicación del ISP el cual es un Netgear.

Gráfica 33: Mapeo general con opción “all”.

```
root@curso:/# nmap -A 192.168.0.22

Starting Nmap 6.00 ( http://nmap.org ) at 2017-10-03 00:42 ART
Nmap scan report for 192.168.0.22
Host is up (0.0037s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE    VERSION
22/tcp  open   ssh        OpenSSH 7.4 (protocol 2.0)
|_ssh-hostkey: 2048 19:eb:f8:97:58:5b:49:82:ee:2a:df:5f:b8:4b:54:92 (RSA)
80/tcp  open   http       Apache httpd 2.4.6 ((CentOS))
|_http-methods: No Allow or Public header in OPTIONS response (status code 403)
|_http-title: Apache HTTP Server Test Page powered by CentOS
587/tcp closed submission
MAC Address: 08:00:27:2B:44:DA (Cadmus Computer Systems)
Device type: general purpose|storage-misc|specialized|WAP|media device|webcam
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (93%), HP embedded (90%), Crestron 2-Series (88%), Netgear embedd
ed (88%), Western Digital embedded (88%), Linksys Linux 2.4.X (86%), AXIS Linux 2.6.X (86%)
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3 cpe:/o:crestron:2_series cpe:/o:linux:kernel:2.6.22 cpe:/o
:linksys:linux:2.4 cpe:/o:linux:kernel:2.4 cpe:/o:axis:linux:2.6
Aggressive OS guesses: Linux 2.6.22 - 2.6.36 (93%), Linux 2.6.39 (93%), HP P2000 G3 NAS device (90%), Linux 3.0
(88%), Linux 2.6.23 - 2.6.30 (88%), Linux 2.6.31 - 2.6.35 (88%), Linux 2.6.9 - 2.6.27 (88%), Crestron XPanel con
trol system (88%), Netgear DGB34G WAP or Western Digital WD TV media player (88%), Linux 2.6.37 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   3.72 ms 192.168.0.22

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.93 seconds
```

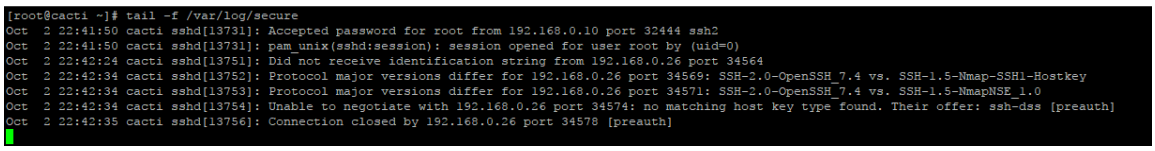
Fuente: El autor.

Finalizando estos escaneos se logró determinar que los únicos puertos y protocolos a su vez habilitados son el puerto 80 de HTTP y el puerto 22 de SSH, este segundo por buenas prácticas debe cambiarse ya que es muy evidente el 22 para ataques a fuerza bruta como se había mencionado previamente, también la modificación del Login del root vía ssh en el mismo archivo de configuración.

Se debe realizar el procedimiento de cambiar el mismo en el archivo /etc/ssh/ssh_config, y robustecer el IPtables del SO.

Antes de proceder a realizar los cambios descritos, se valida el log de secure del SO en el apache, en el /var/log/secure:

Gráfica 34: Validación del log de seguridad del SO.

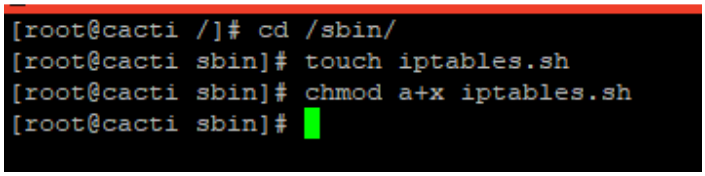


Fuente: El autor.

Y efectivamente se detectan los escaneos desde el host atacante:

El procedimiento para cerrar el IPtables se realiza con el siguiente script:

Gráfica 35: Creación de script para corrección IPtables.



Fuente: El autor.

Gráfico 36: Script.

```
#!/bin/bash

iptables -F

iptables -A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 9122 -j ACCEPT
iptables -A INPUT -s 181.56.69.152 -p tcp -m tcp --dport 10050 -j ACCEPT
iptables -A INPUT -s 181.56.69.152 -p tcp -m tcp --dport 10051 -j ACCEPT
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp -m tcp ! --tcp-flags FIN,SYN,RST,ACK SYN -j REJECT --reject-with tcp-reset
iptables -A FORWARD -m state --state INVALID -j DROP
iptables -A FORWARD -i lo -o lo -j ACCEPT
iptables -A FORWARD -j DROP
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp ! --tcp-flags FIN,SYN,RST,ACK SYN -j REJECT --reject-with tcp-reset
iptables -A OUTPUT -m state --state INVALID -j DROP
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp -m tcp ! --tcp-flags FIN,SYN,RST,ACK SYN -j REJECT --reject-with tcp-reset
iptables -A INPUT -m state --state INVALID -j DROP
iptables -P FORWARD DROP

service iptables save
~
```

Fuente: El autor.

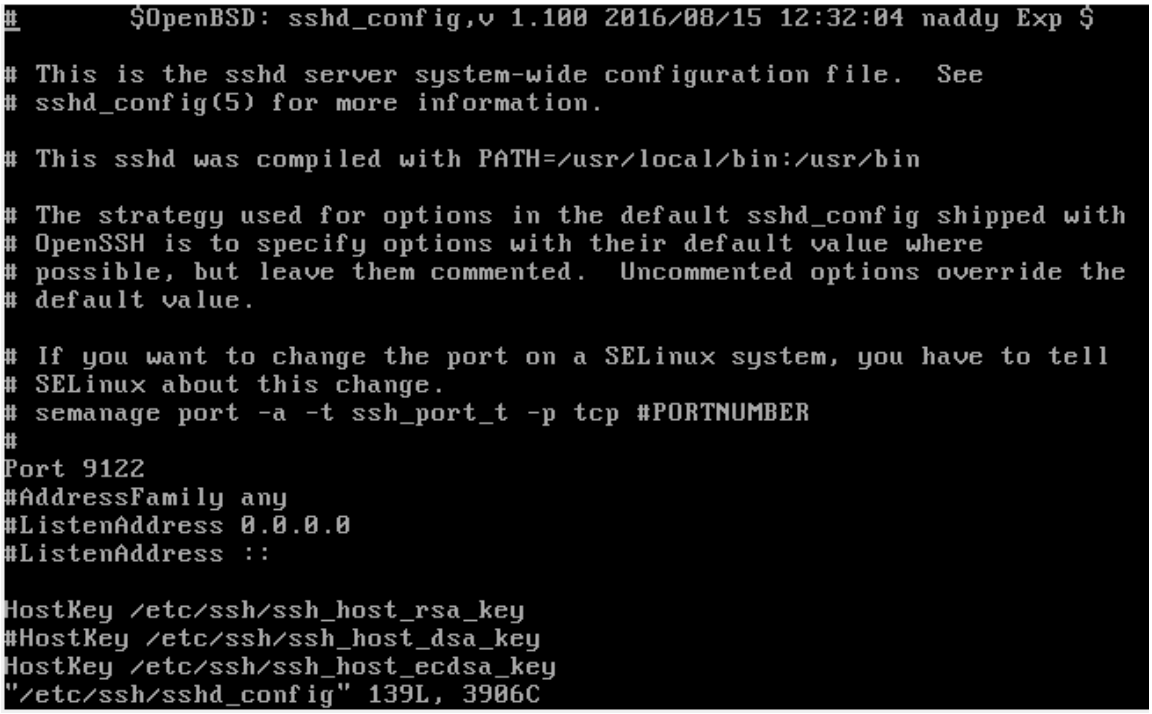
Gráfica 38: Ejecución y validación de script.

```
[root@cacti sbin]# ./iptables.sh
The service command supports only basic LSB actions (start, stop, restart, try-restart, reload, force-reload, status).
[root@cacti sbin]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:smtp
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:grcmp
ACCEPT     tcp  --  static-ip-1815669152.cable.net.co  anywhere            tcp dpt:zabbix-agent
ACCEPT     tcp  --  static-ip-1815669152.cable.net.co  anywhere            tcp dpt:zabbix-trapper
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
REJECT     tcp  --  anywhere             anywhere            tcp flags:!FIN,SYN,RST,ACK/SYN reject-with tcp-reset
DROP       all  --  anywhere             anywhere            state INVALID

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
REJECT     tcp  --  anywhere             anywhere            tcp flags:!FIN,SYN,RST,ACK/SYN reject-with tcp-reset
DROP       all  --  anywhere             anywhere            state INVALID
ACCEPT     all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
REJECT     tcp  --  anywhere             anywhere            tcp flags:!FIN,SYN,RST,ACK/SYN reject-with tcp-reset
DROP       all  --  anywhere             anywhere            state INVALID
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD_IN_ZONES (0 references)
target     prot opt source               destination

Chain FORWARD_IN_ZONES_SOURCE (0 references)
target     prot opt source               destination
```

Fuente: El autor.

Posterior a este script se realizan los ajusten en el archivo de configuración del SSH como se había planteado previamente. Modificación del puerto 22 y el bloqueo del login del root:

Gráfica 38: Modificación de Puerto a 9122.

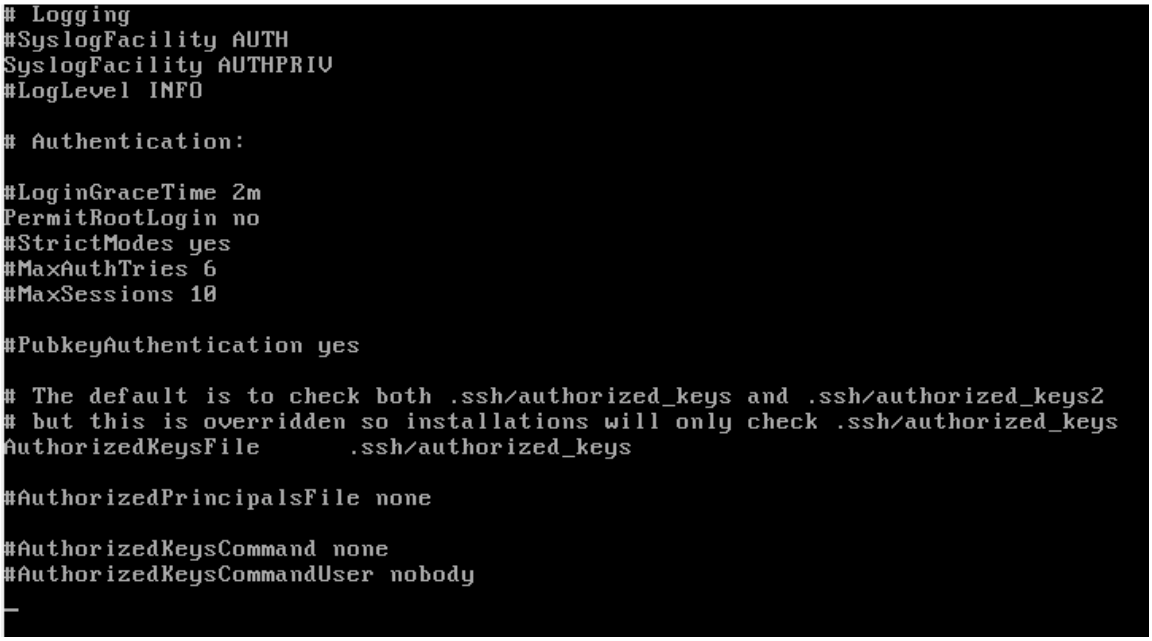


Fuente: El autor.

La modificación del login del root vía ssh se realiza para eliminar ataques de fuerza bruta tipo diccionario con el usuario root. Además permite tener un paso más de autenticación al sistema operativo ya que el usuario regular aparte de logearse ssh si desea ejecutar funciones de root deberá elevar su perfil, si no tiene esta contraseña de root no podrá hacer cambios algunos. Esto acorde a buenas practicas a nivel de perfiles horizontales y verticales.

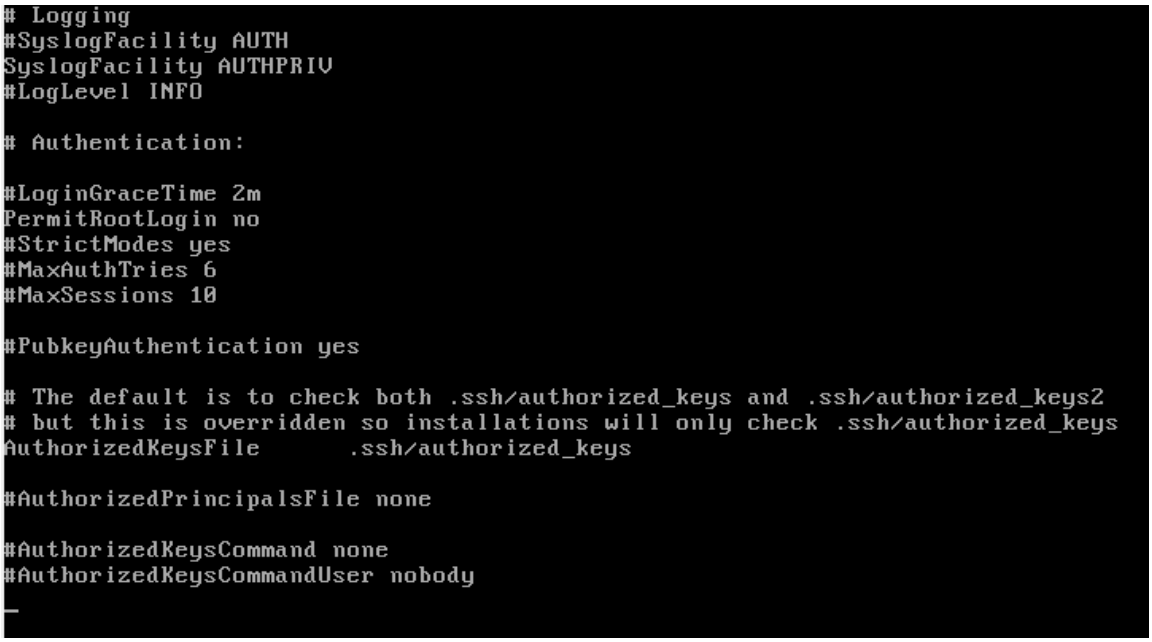
La edición del archivo es la siguiente:

Gráfica 39: Deshabilitar la autenticación root vía ssh.



Fuente: El autor:

Gráfica 40: Modificación de autenticación del root vía SSH.



Fuente: El autor.

Después de haber efectuado las correcciones y salvado los cambios del IPtables se procede a realizar un mapeo completo.

Gráfica 41: nmap –all.

Fuente: El autor.

Con esto se comprueba que exclusivamente se deja habilitado el puerto 80 de http.

Después de estas pruebas realizadas para la capa media y su respectiva corrección de errores, procedemos a apuntar a la capa de host con MetaExploit. Para ello se utiliza una herramienta llamada Kali Linux.

Con la misma descargar una herramienta llamada Pentmenu y con esta realizar un ataque de denegación de servicio DoS, por la IP LAN, y apuntando al único puerto en el IPtables publicado que es el 80 del HTTP, se realizará un ataque por más de 1 hora de peticiones que llegarán a una cantidad de 10 millones.

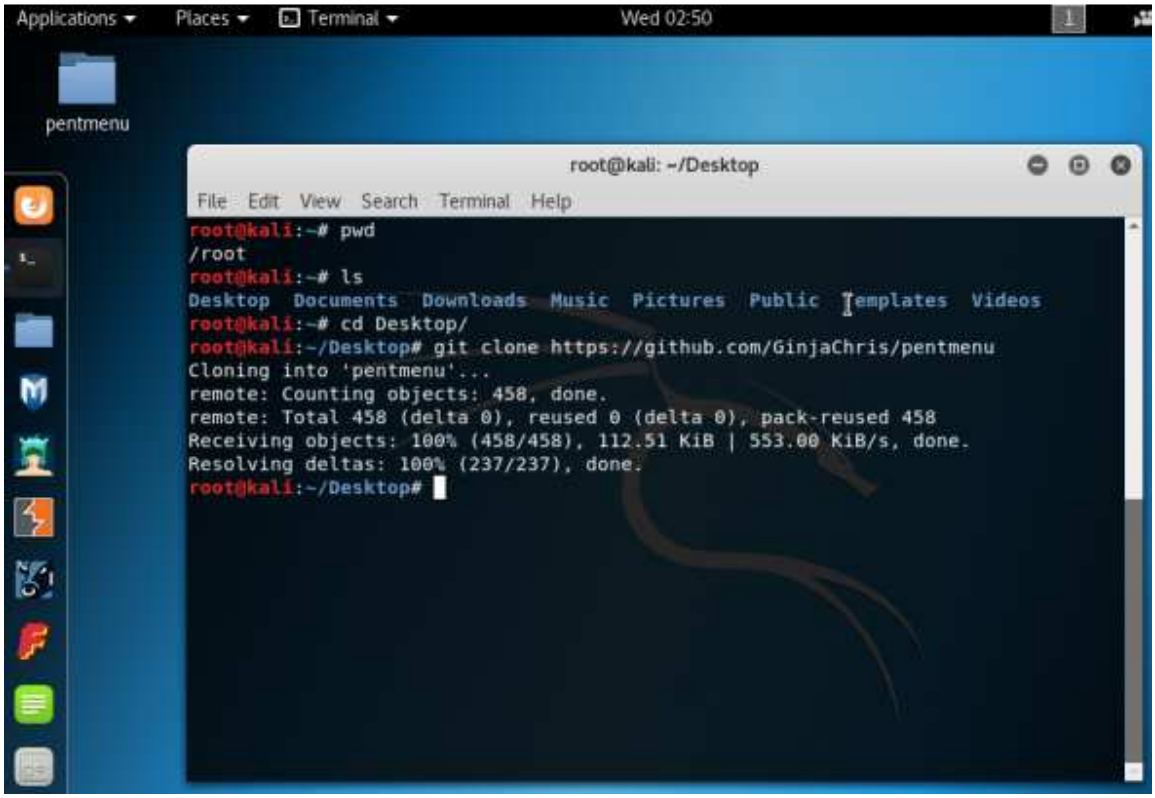
Si el WAF Mod_Security no está configurado correctamente el servicio de Apache se caerá después de efectuar tantas respuestas a dichas peticiones vía TCP.

El procedimiento a realizar es el siguiente:

Ubicar en el Dekstop del usuario del Kali Linux y descargar a través de GitHub la herramienta pentmenu, esta herramienta permite generar varios tipos de ataques, en este caso vamos a enfocarnos a ataques de tipo DDoS (denegación de servicio). En este documento lo llamaremos DoS.

A continuación en la gráfica 42 se describe la descarga de la herramienta:

Gráfica 42: Descarga de pentmenu.



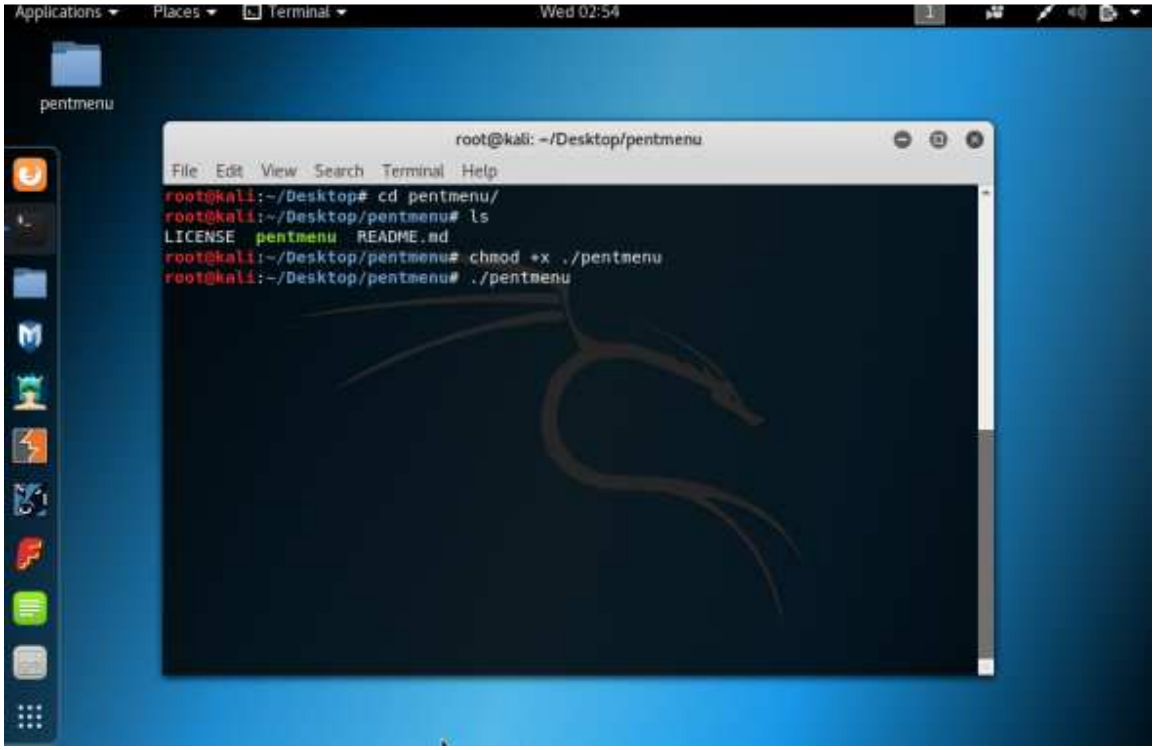
Fuente: El autor.

Posterior a esta descarga se procede a ir al repositorio de pentmenu y configurar el script agregando el bit de ejecución (x= excecute), para así de esta manera lograr ejecutar el software de manera local.

Recordemos que en Linux la ejecución de los archivos debe tener el permiso octal adicionando X (R= read, W= Write, X= execution).

La gráfica 43 demuestra el cambio de permisos:

Grafica 43: Ejecución pentmenu.



Fuente: El autor.

Después de haber ejecutado el mismo el software a través de un menú nos pedirá algunos parámetros de configuración para ejecutar el ataque de denegación de servicio o como se llama técnicamente DDoS pero en este documento lo llamaremos DoS debido a que así aparece en la herramienta.

Para esta ocasión se escogerá la opción dos (2) y dar ENTER.

Grafica 44: Ejecución de la opción DoS.

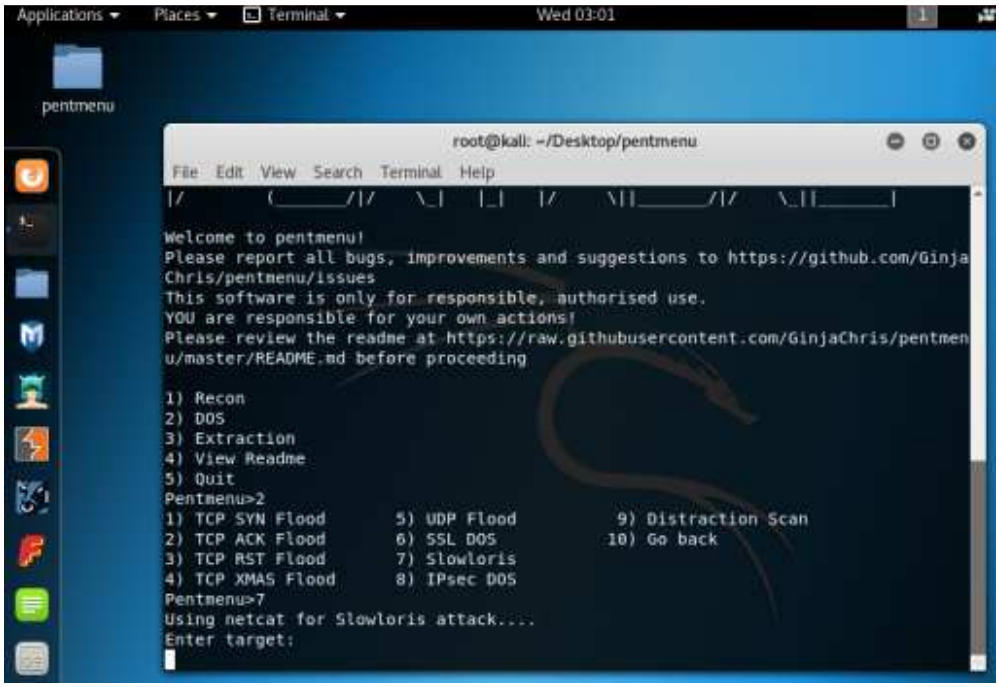
Fuente: El autor.

Luego de haber seleccionado la opción de DoS, el software nos solicitará el método a utilizar para dicho ataque, en este caso la opción es Sloworis; esta es una herramienta de denegación de servicio inventada por Robert Hansen “Rsnake” en el año 2009 la cual permite a un solo equipo de cómputo, en este caso el Kali Linux derribar a un servidor web con un ancho de banda mínimo. Esta herramienta permite mantener abiertas muchas conexiones al servidor Apache (en este caso el que tiene instalado el Mod_Secutiry) y enviando una petición parcial de manera periódica enviando los encabezados HTTP, añadiendo de manera parcial pero nunca completando la solicitud. Lo cual haría que el servidor Apache vaya llenando su número máximo de conexiones hasta caerse.

Recordemos que el protocolo HTTP es nativo vía TCP, a esto nos referimos que es un protocolo de envío y respuesta del mismo, al enviarse un número X de peticiones el HTTP responderá una por una hasta llegar a un límite determinado, en el cual ya no atenderá más solicitudes y se caerá el servicio; esto si no se tiene configurado un WAF que rechace las peticiones que detecte como falsas y/o inseguras.

En este caso solo basta con colocar el target ósea el objetivo, identificado por la IP, el protocolo que es HTTP puerto 80 y la cantidad de peticiones que vamos a enviar en este caso 10’000.000, de la siguiente manera:

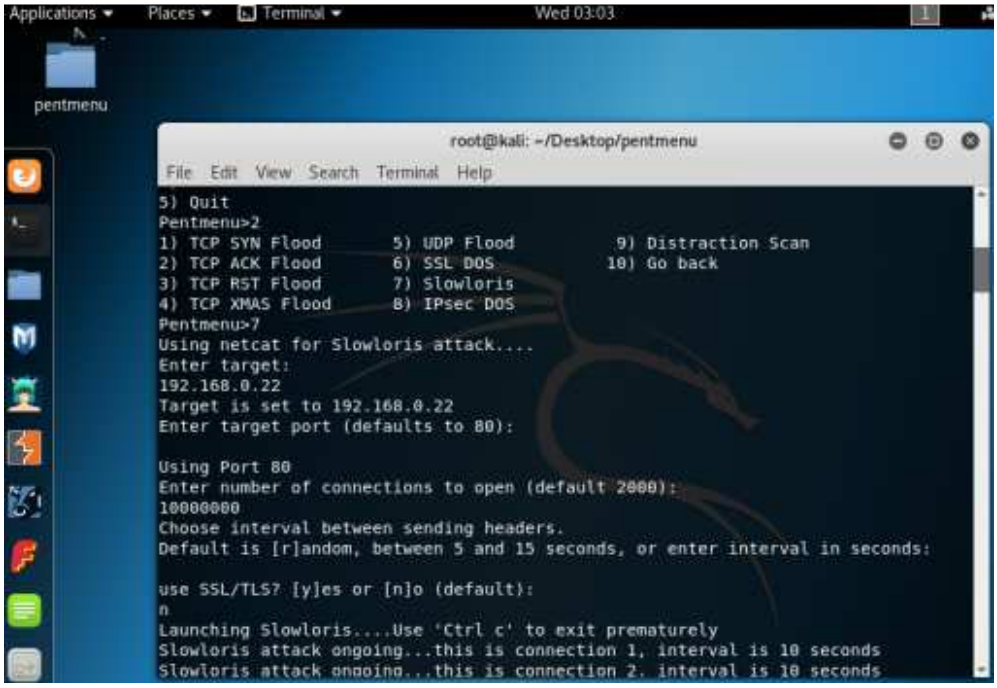
Grafica 45: Configuración de apuntamiento DoS.



Fuente: El autor.

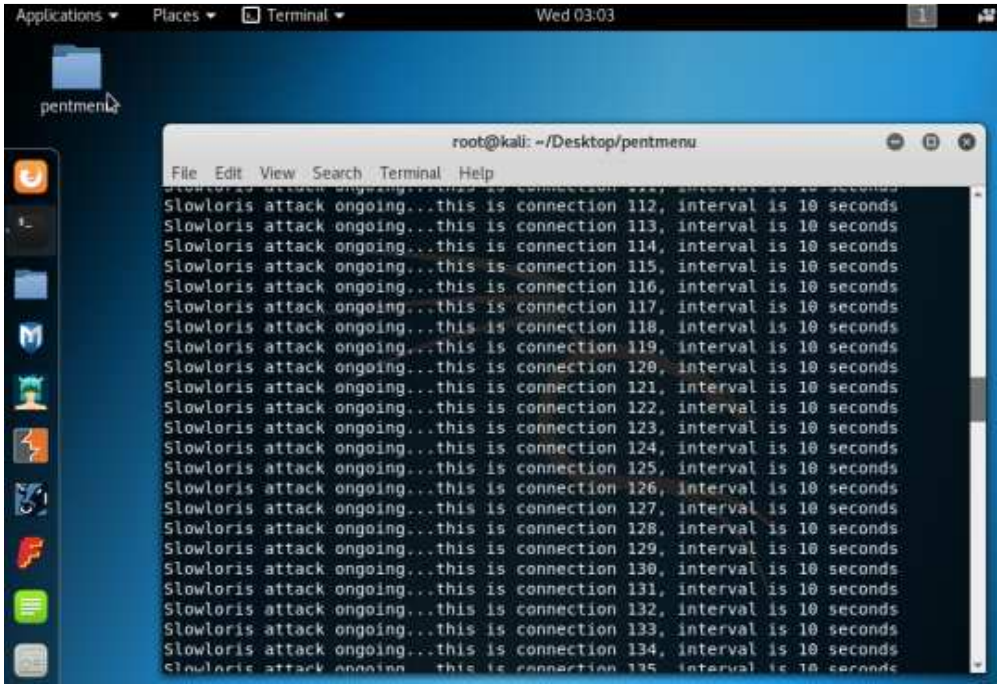
Este ataque enviará 10 millones de peticiones a 1 solo servidor apache, sin balanceador de carga y tan solo con un WAF instalado, en este caso el Mod_Secutiry. Las peticiones HTTP enviadas son peticiones inconclusas que solo envían el headers de manera subsecuente pero no completa con tal de mantener la mayor cantidad de tiempo la petición abierta o sesión como se llama en Apache, algo muy similar a un TTL Time to life. Esto con tal de mantener un tiempo mayor las peticiones antes que el apache las descarte y las rechace el WAF. Así en algún momento de los 10 millones de peticiones enviadas una cantidad importante estará solicitando respuesta del apache y probablemente se caiga el servidor. Dependiendo de las buenas practicas utilizadas en el WAF se caerá o no el servidor.

Grafica 46: Enviando ataques DoS.



Fuente: El autor.

Gráfica 47: Enviando Peticiones.



Fuente: El autor.

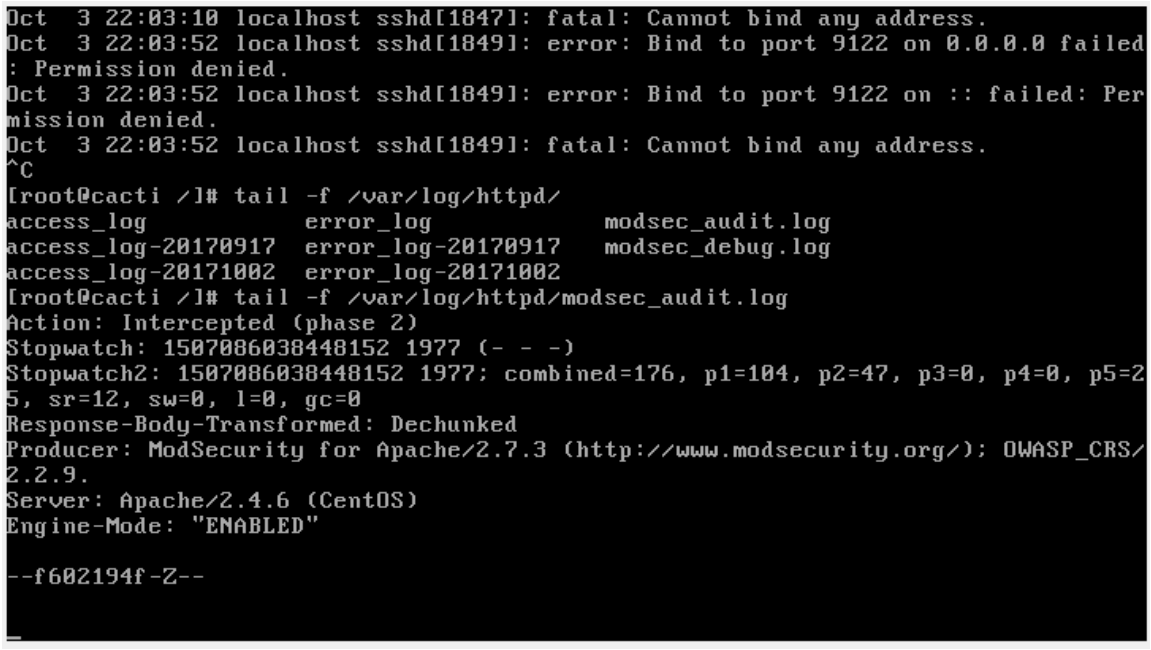
Después de una hora de envío de 10’000.000 de peticiones el servidor Apache no se ha caído aun, debido a que su configuración de integración del WAF Mod_Secutiry junto al HTTP Apache, logra determinar que es un ataque tipo inteligente de denegación de servicio y procede a descartar dichas peticiones, esto se puede validar en el log de eventos del Mod_Secutiry de la siguiente manera:

Tail –f /var/log/http/modsec_audit.log

En el mismo se logra ve el stopwatch de peticiones, o más bien la detención de respuestas a estas solicitudes enviadas por el Kali Linux. Lo cual descarta dichos paquetes a nivel de capa de aplicación si pensamos en el modelo OSI y capa de Host si tomamos en cuenta esta segunda prueba realizada a nivel de análisis de vulnerabilidad.

A continuación el log de eventos:

Gráfica 48: Log del WAF.



Fuente: el autor.

Finalmente para ver si nuestro apache se cayó desde la perspectiva del cliente o usuario final quien no tiene acceso a ver los logs del sistema operativo, se procede

acceder al browser y apuntar a la IP atacada y se denota que el servicio HTTP es correcto.

Grafica 49: Validación de HTTP vía Browser.

Fuente: El autor.

9. RECOMENDACIONES POSTERIORES AL ANÁLISIS.

En el presente proyecto que corresponde el robustecimiento de una red lan corporativa, en muchas organizaciones cuando se ha tomado la decisión de realizar una inversión a nivel de seguridad informática en su entorno, se opta por cubrir una parte de la topología, comúnmente la más importante o la que esté más expuesta, sin embargo no se realiza una segmentación de manera lógica y a su vez física de lo que comprende a su totalidad.

El tan solo cuantificar la cantidad de dispositivos en la organización de manera individual que tienen acceso a los recursos de la organización y/o tienen consumo desde internet hacia los mismos, podríamos hacernos una idea de que tan vulnerable es cualquier red corporativa.

Es muy complicado garantizar la seguridad de cada uno de los elementos previamente mencionados de manera individual. Por lo tanto debemos pensar de una manera más macro, en la cual podamos tener todos esos elementos, servicios, consumos y demás y catalogarlos en categorías a nivel de conectividad y enfocar nuestros esfuerzos en robustecer dichas categorías.

Para lo previamente descrito se ha optado por catalogar nuestros servicios en el modelo OSI, recordemos la definición del modelo OSI:

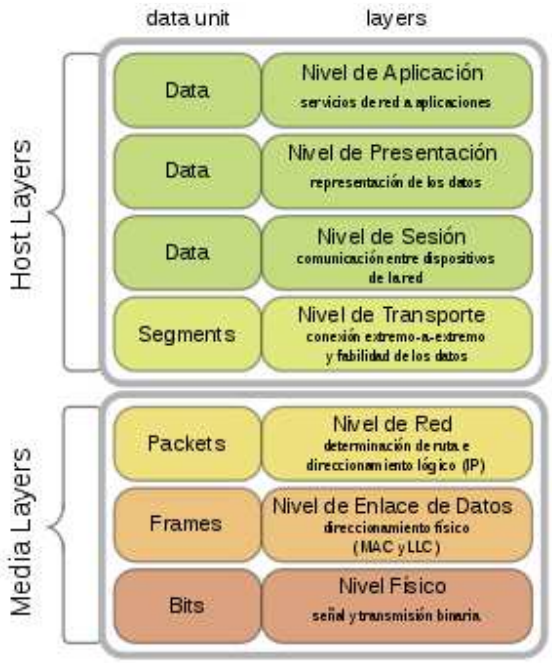
Este se llama modelo de interconexión de sistemas abiertos (ISO/IEC-7498-1), el cual referencia los protocolos de arquitectura de red en siete capas las cuales a su vez de manera lineal son fases por las cuales deben pasar los datos de un dispositivo de comunicación a otro en una red de comunicaciones.

Por medio de este modelo OSI, y enfocado a cada una de sus siete capas podemos correlacionar los elementos de nuestra organización y acorde a su naturaleza; ejemplo: Capa de aplicación – antivirus. Brindar una solución de robustecimiento en la red lan corporativa.

Pero el hecho de asociar cada uno de nuestros servicios y/o componentes a las siete capas del modelo OSI hace un poco extenso y de cierta manera compleja su asociación, además hay capas que no aplican, por ejemplo; capa de sesión, se sabe que ésta está enfocada a controlar el diálogo entre los servicios a nivel de capa de aplicación en lo cual es la naturaleza del protocolo TCP/IP, esto y las variables de sesión en capa 7.

Por lo tanto y en base a lo anterior se toma la decisión de tomar estas siete capas del modelo OSI y dividirlas en dos de la siguiente manera:

Gráfica 50: Subdivisión capas modelo OSI.



Fuente: https://es.wikipedia.org/wiki/Modelo_OSI

Esta subdivisión en dos capas, las cuales son capa de host y capa media, permite realizar un enfoque de una manera más resumida y asociativa, de igual manera catalogar cada uno de los elementos que comprende la organización a este modelo y así establecer las mejores prácticas en lo que refiere al robustecimiento de cualquier red corporativa.

En el desarrollo del presente proyecto y acorde a las pruebas realizadas, se concluye de los resultados evidenciados en las dos capas previamente descritas así como las respectivas correcciones. Primeramente la capa Media, la cual comprende el nivel físico, enlace de datos y nivel de red, se puede considerar esta como una asociación de servicios de networking y físicos. En primera medida y acorde al primer objetivo específico del mismo se realizó la actualización de licencias, firmwares, y software que comprenden los appliances, esto enfocado en este proyecto puntualmente al firewall (en este caso Sonicwall), recordemos que como buena práctica al tener este tipo de licenciamiento al día el fabricante nos enviará actualizaciones a nivel de seguridad, fixes y correcciones. Esto a lo que

refiere a appliances. Ahora en lo que se centra a networking se realizaron en los mismos appliances listas de control de acceso (ACL) las cuales de manera mandatoria permiten, rechazan o deniegan el paso de servicios, protocolos y/o puertos a la red, dejando solo acceder y salir los que son estrictamente necesarios.

Ahora las pruebas realizadas de vulneración comprendieron efectuar mapeos de diferente manera a la red con tal de evidenciar puertos y/o servicios vulnerables, las correcciones fueron efectuadas de maneras satisfactorias.

Pero estas vulnerabilidades solo fueron validadas a nivel de networking, ya que esta capa se enfoca en esta naturaleza, posterior a la misma se efectuó modificaciones y mejoras a la capa de Host la cual comprende las siguientes; capa de aplicación, nivel de presentación, nivel de sesión y nivel de transporte.

Esta capa de host enfocada un poco más a nivel de aplicación y software, fue robustecida por medio de configuraciones del firewalls internos, actualización y licenciamiento de antivirus, instalación de parches se seguridad y corrección de fixes a nivel de sistemas operativos, configuración e instalación de plugins de web browser en equipos clientes.

Una de las pruebas realizadas con Kali Linux se evidenció fallas y falencias a nivel de aplicación de los sistemas operativos, como puertos de ssh por default y permisos para conexión y autenticación de usuarios root sobre servidores de consumo tipo web service. Fallas que posteriormente fueron corregidas además de ellos se aprovechó y se instaló un firewall inteligente llamado WAF o como traduce su nombre al español Firewall de Aplicación Web, el cual va un poco más allá y de manera inteligente y con a prendimiento supera las configuración de un firewall normal como el de la capa media, ya que este contiene triggers, los cuales permiten identificar y contener ataques de tipo robot, sql injection y demás, en este caso probamos puntualmente con ataques de DoS, los cuales normalmente ejecutan robots de manera coordinada y centralizada a un objetivo en común, los resultados de estas pruebas fueron satisfactorios.

En resumen se logró efectuar varias mejoras en lo que comprende a la organización a nivel de infraestructura en cada una de las capas del modelo OSI, robusteciendo así a red lan corporativa.

Pero aun así sin embargo y acorde a las buenas prácticas se debe actualizar permanentemente las versiones de sistemas operativos, licenciamiento, configuraciones, actualizaciones de parches y fixes y políticas de seguridad en las

consolas antivirus para que el margen de vulnerabilidad sea mucho menor, casi nulo.

Para ello se sugiere realizar revisiones contantes a todos los sistemas de información previamente descritos.

9.1 RECOMENDACIONES

Acorde al robustecimiento de la red LAN corporativa realizado previamente en base al modelo OSI se dio solución a varios conceptos de ingeniería tales como dispositivos que comprenden la capa media, está refiriéndose a capas de networking y dispositivos de capa de host ésta refiriéndose a la capa de aplicaciones. Además de ello complementando con capacitaciones a nivel de seguridad informática a los empleados de la empresa haciéndoles entender la importancia que comprende la información, su uso, disponibilidad y fiabilidad.

Se recomienda establecer un modelo en base a la norma ISO 27002 la cual refiere a establecer un catálogo de buenas prácticas que se determinan no solo en base de la experiencia del ingeniero de seguridad informática sino que se apoya en una serie secuencial de objetivos de control, controles y demás que se integran en la norma 27001 en lo que refiere al tratamiento de riesgos.

Dicha norma ISO 27002 descrita en 14 capítulos las cuales de manera explícita refieren las áreas en las cuales se debe a garantizar el robustecimiento de la red LAN corporativa enfocada a un plan de seguridad informática en la organización, dicho documento realiza recomendaciones de controles para tener en cuenta en el cumplimiento de la organización, un total de 114. No es necesario cumplirlos todos pero si son una guía para el cumplimiento de la norma.

Dentro de los controles que se recomienda de la norma ISO 27002 se realiza la sugerencia con respecto a los siguientes a aplicar en la organización:

- Seguridad Física y entorno.
- Seguridad de las operaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Aspectos de seguridad de la información para la gestión de la continuidad de negocio.

Las previamente descritas complementarían no solo el robustecimiento de una red LAN corporativa sino orientarían a la organización a pensar en la implementación de un SGSI, llegando a un nivel de madurez en la misma en la a la cual toda empresa quiere llegar en lo que refiere a seguridad informática.

CONCLUSIONES

El mayor valor que tiene cada organización es la información, este es el principal activo de la misma, su eje fundamental y la manera por la cual la misma subsiste sin importar la naturaleza de esta. Los tres pilares de la seguridad informática enuncian que este activo; la información debe ser confidencial, integra y conservar su disponibilidad. En base a eso es primordial actuar de manera proactiva antes que reactiva, referente a establecer buenas prácticas en el funcionamiento y configuración a lo que respecta a los elementos que se encargan de manipular la información.

Es importante tener a un personal capacitado de colaboradores para que estos tengan conocimiento de lo importante que es la información y de lo crítico que puede llegar a ser si esta se altera, se viola, se sustrae o se afecta de alguna manera ya se intencional o no intencional. También enfocándose en lo que se llama ingeniería social, una técnica muy utilizada por atacantes los cuales se enfocan en cualquier miembro de la organización para realizar un bosquejo de lo pueden llegar encontrar y la técnica a utilizar, después de haber sustraído información.

Debe establecerse buenas prácticas a nivel de configuración y arquitectura de la seguridad en la infraestructura tecnológica de la organización, esto resumido en un robustecimiento en la red LAN corporativa, en la cual no solo se realiza la configuración necesaria de los equipos y dispositivos de información, si no que se establecen buenas prácticas, enfocado en la conducta que refiere a una mayor capacidad de seguridad corporativa y constante monitoreo de la misma, enfocándose en minimizar lo mayor posible una afectación a los servicios de información si en dado caso ocurre, esto basado en conceptos de ingeniería como es el tomar cada uno de los elementos de la misma y asociarlos a una capa del modelo OSI y robusteciendo la misma logrando de esta manera parametrizar varios conceptos e ítems que se encuentran en niveles similares y darles una solución debida.

Además de este robustecimiento a nivel lógico se debe establecer la buena práctica del tener actualizado los sistemas operativos, licenciamiento y appliances de la organización, esto debido a que los fabricantes se preocupan por tener de manera actualizada sus librerías de datos en cuento a malwares. Esta buena práctica conlleva a un riesgo menos en la organización el cual son los fixes y

parches de seguridad que corrigen vulnerabilidades encontradas en la organización.

Para finalizar además de realizar todas las labores enunciadas previamente lo más importante es que el personal de TI encargado de seguridad informática esté en constante capacitación y actualización, de esta manera día a día se pueden encontrar más y mejores maneras de mejorar la seguridad de la red, y siendo más proactivos que reactivos en el momento de afrontar las amenazas constantes que se pueden presentar a nivel de malwares y/o nuevos ataques en el mundo informático.

DIVULGACIÓN

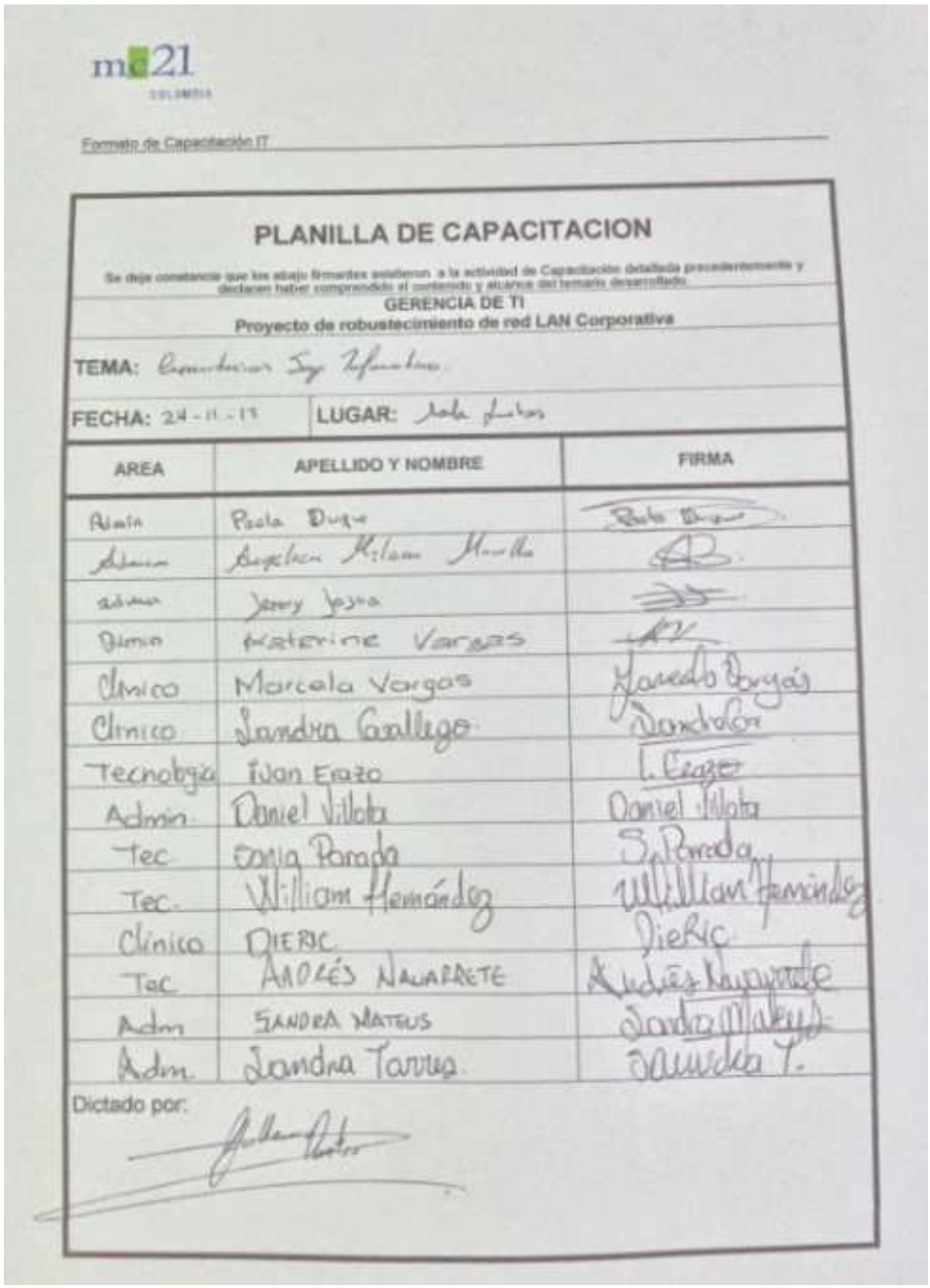
Es muy importante realizar el proceso de divulgación a los empleados y colaboradores del robustecimiento de la red LAN corporativa, ya que debe ser de común entendimiento entre la dirección de la organización y/o junta directiva y a su vez cada uno de los empleados, y comprender que este proceso de robustecimiento no solo implica todo lo referente a ingeniería sino también la colaboración de los mismos empleados, ya que de ellos también comprende la seguridad de la información como lo son los documentos físicos, facturas, portabilidad de equipos de cómputo y demás.

De acuerdo a lo anterior se realiza una capacitación a los empleados en el cual se les describe los riesgos y posibles ataques a los cuales se encontrarán en cualquier momento, no solo informáticos sino los que se realizan por medio de ingeniería social; de personas externar a la organización como lo puede ser la competencia empresarial, un hacker profesional o alguna persona que pueda mediante algunas preguntas sencillas, consideradas de rutina envolver a cualquier colaborador con el fin de sacar información que pueda servir para un siguiente ataque informático, esto anteriormente descrito considerado como Ingeniería Social.

En el mismo proceso de capacitación se realiza una breve descripción a lo que refieren las listas de control de acceso (ACL) las cuales están catalogadas por áreas, asociadas a usuarios y estos a contenidos web. No solo evitan el acceso a sitios no permitidos sino a la optimización del ancho de banda de la organización enfocando sus recursos de conectividad a sitios que son netamente necesarios para las actividades relacionadas con el trabajo e investigación.

A continuación se inserta el documento de la organización que refiere a este tipo de capacitaciones:

Gráfica 51: Planilla de capacitaciones.



Formato de Capacitación IT

PLANILLA DE CAPACITACION

Se deja constancia que los abajo firmantes asistieron a la actividad de Capacitación detallada precedentemente y declaran haber comprendido el contenido y alcance del temario desarrollado.

GERENCIA DE TI

Proyecto de robustecimiento de red LAN Corporativa

TEMA: Generalidades Sys Informáticos

FECHA: 24-11-15 **LUGAR:** Sala Juntas

AREA	APELLIDO Y NOMBRE	FIRMA
Admin	Paola Duque	
Admin	Angelica Milena Murillo	
Admin	Jenny Jesus	
Admin	Katerine Vargas	
Clinico	Marcela Vargas	
Clinico	Sandra Gallego	
Tecnología	Juan Erazo	
Admin	Daniel Villota	
Tec	Sonia Pareda	
Tec.	William Hernández	
Clinico	DIERIC	
Tec	ANDRÉS NAVARRETE	
Adm	SANDRA MATEUS	
Adm	Sandra Tarres	

Dictado por:

Fuente: El autor.

BIBLIOGRAFÍA

Nivel Nacional, Ley 1273 de 2009, Artículo 1. 15/07/2018. [En línea]. Enero 5 del 2009. [Citado 15-Jul-2018]. Disponible en:

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Soluciones TIC, Ley 603 de 2000, 15/07/2018. [En línea]. Enero 2016. [Citado 15-Jul-2018]. Disponible en:

http://www.e-solucionestic.com/ley-603-del-2000/

Redipd, Ley Estatutaria 1266 del 31 de Diciembre del 2008, Artículo 4° sección B.

[En línea]. Diciembre 31 del 2008. [Citado 15-Jul-2018]. Disponible en:

http://www.redipd.org/legislacion/common/legislacion/Colombia/LEY_1266_31_12_2008_HabeasData_COLOMBIA.pdf

Secretaría Jurídica Distrital, Ley 1273 del 5 de Enero del 2009, Capítulo 1. [En línea]. Enero 5 del 2009. [Citado 15-Jul-2018]. Disponible en:

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

MinTIC, Ley 1341 del 30 de julio del 2009. Capítulo 1. [En línea]. Junio 10 del 2018. [Citado 15-Jul-2018]. Disponible en:

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Secretaría Jurídica Distrital, Ley 599 de 2000. Artículo 195. [En línea]. Julio 24 del 2000. [Citado 15-Jul-2018]. Disponible en:

http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Adbisera Expert Solution, NORMA ISO/IEC 27001:2013. [En línea]. Enero 2 del 2018. [Citado 15-Jul-2018]. Disponible en:

https://advisera.com/27001academy/es/que-es-iso-27001/

CARDONA, Juan David. (2013). Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda [En línea]. 2017. [Citado 22-May-2017].Disponible en internet: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

CHILAN, Leslie. Análisis para integración de un Sistema de Gestión de Seguridad de la Información (SGSI) ISO-27001 utilizando OSSIM. [En línea] 2014. [Citado 17-Jul-2017] Disponible en internet: http://dspace.ups.edu.ec/bitstream/123456789/7401/1/UPS-GT000773.pdf

ISO/IEC TR 18044:2004. Information Technology, Security Techniques, Information Security Incident Management. ISO. Octubre de 2004 [En línea]. https://www.iso.org/standard/35396.html

MURILLO, Estefanie. Diseño de una metodología para la implementación del Sistema De Gestión De Seguridad De La Información. [En línea] 2012. [Citado 13-Jul-2017] Disponible en: http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf

NTC, Norma técnica Colombiana [En linea]. 2006 [Citado Mayo 22 de 2017] Disponible en internet:

http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

RIBADAS, Explotación de Vulnerabilidades: uso básico de Mestasploit [En línea] http://ccia.ei.uvigo.es/docencia/SSI-grado/1314/practicas/uso-metasploit/index.html

Implementación de Windows Server Update Services en una organización. [En línea]. [Citado 15-Jul-2018]. Disponible en:

https://msdn.microsoft.com/es-es/library/hh852340(v=ws.11).aspx

MaAfee ePolicy Orchestrator 5.3.0 - Software Guía del producto. Configuración de producto. [Citado 15-Jul-2018]. Disponible en:

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25504/es_ES/epo_530_pg_0-02_es-es.pdf

Knowledge Center Mc Afee- Acceso a configuración de base de datos EPO Mc Afee. Configuración de producto. [Citado 15-Jul-2018]. Disponible en:

https://kc.mcafee.com/corporate/index?page=content&id=KB51465

DELL, Manual de configuración SonicWall referencia TZ500, [Citado 15-Jul-2018]. Disponible en:

https://downloads.dell.com/rdoc/dell%20sonicwall%20tz500%20w,apl29-0b7,n_a,dell%20regulatory%20and%20environmental%20datasheet.pdf

Oracle Enterprise Linux, Licenciamiento y actualización de parches, [Citado 15-Jul-2018]. Disponible en:

http://www.oracle.com/us/technologies/027617.pdf

ModSecurity Handbook, Getting Started - Release 15 de Julio del 2017. [Citado 15-Jul-2018]. Disponible en:

https://www.feistyduck.com/books/modsecurity-handbook/gettingStarted.html