Diseño y simulación de una infraestructura de red segura

Víctor Pliego García

Resumen– En la actualidad estamos viviendo a una revolución que está provocando grandes cambios en nuestra sociedad. Internet cada vez está más presente en nuestro día a día trayendo consigo grandes ventajas y desventajas.

Es por ello que la seguridad está empezando a adoptar un papel muy importante en el sector empresarial. En este proyecto se implementará seguridad en las diferentes capas de una infraestructura de red: en el diseño de la red interna, en los firewalls, en los servicios que ofrece y en su monitorización.

Palabras clave– Internet, seguridad, red, firewall, servidor, servicio, iptables, infraestructura, port knocking, VPN, vulnerabilidad, DMZ, log.

Abstract– Nowadays we are living a revolution that is causing big changes in our society. Internet is increasingly its presence in our day to day bringing great advantages but great disadvantages too.

That is why the security is beginning to take a very important role in the business sector. This project will implement security in the layers of the network infrastructure: in the design of the local area network, in firewalls, in the services offered and in their monitoring.

Keywords– Internet, security, network, firewall, server, service, iptables, infrastructure, port knocking, VPN, vulnerability, DMZ, log.

1 Introducción

Los seres humanos siempre hemos tenido la necesidad de comunicarnos los unos con los otros, ya sea utilizando nuestro propio cuerpo, elementos que nos rodean e incluso entidades que no podemos siquiera ver.

Hasta hace unas décadas, la comunicación entre humanos era lenta y los medios de los que se disponían no permitían que la velocidad y calidad de la comunicación avanzara.

A raíz de la aparición de Internet y de las nuevas técnicas de comunicación que han ido surgiendo, se ha facilitado la interconexión de las personas y las máquinas, creando un mundo virtual con millones de datos a nuestro alcance. Surge entonces, la necesidad de proteger esos datos y los sistemas que los contienen.

Cuando vivimos en un mundo interconectado y rebosante de información, aparecen, como en todos los ámbitos de la vida, personas u organizaciones que tratan de aprovecharse de los resquicios y brechas del sistema establecido utilizando técnicas maliciosas. Cuando se dan este tipo de prácticas se recurre a la implantación de contramedidas para evitar este tipo de acciones. Es a partir de la "mala" praxis por parte de un sector de Internet, cuando se aplica una capa de seguridad extra a los sistemas y conexiones de la infraestructura de red.

El proyecto consiste en el diseño y creación de la estructura de red de una empresa con dos sedes y de garantizar su seguridad. Para empezar, se realiza una primera búsqueda para analizar el estado del arte actual y las tecnologías más utilizadas y extendidas a día de hoy en las infraestructuras de redes empresariales. Seguidamente, se aplican algunas de estas tecnologías en el diseño, simulación, seguridad de la integridad y privacidad de la red. A continuación, con la red de la empresa ya interconectada y ofreciendo un flujo de datos, se monitoriza y se analiza el tráfico de la red. También se analizan y se ponen en práctica las vulnerabilidades que podrían aprovecharse para ver comprometida la seguridad de una máquina. Finalmente se realizarán un conjunto

• E-mail de contacte: victor.pliego@e-campus.uab.cat
• Menció realitzada: Tecnologies de la Informació
• Treball tutoritzat per: Juan Carlos Sebastián Pérez (dEIC)
• Curs 2016/17

de pruebas y demostraciones de todas las tecnologías utilizadas para analizar y explicar el resultado obtenido.

2 OBJETIVOS

- Diseño del diagrama de infraestructura de red de la empresa.
- Monitorización y análisis del estado normal de la red local y sus servicios
- Creación de firewalls y DMZ.
- Creación de VLAN's.
- Análisis de vulnerabilidades.
- Implementación de sistema de detección de intrusos.
- Balanceo de carga de los servicios internos.
- Backups en red.
- Monitorización y detección intrusiones.

3 ESTADO DEL ARTE

Desde la Aparición de Internet y su uso de forma masiva hasta el día de hoy, la seguridad en los sistemas informáticos ha ido tomando más importancia debido a la gran afluencia de usuarios que utilizan Internet. El masivo uso de Internet ha provocado que en la red fluyan y se transmitan una gran cantidad de datos que se almacenan en servidores.

Conforme Internet ha ido creciendo han surgido compañías tecnológicas que gracias a las facilidades y servicios que ofrecen a los usuarios se han convertido en imprescindibles en el día a día de los usuarios.

Hasta ahora se ha hablado sobre las empresas tecnológicas punteras de hoy en día, pero no se debe olvidar a las empresas que pertenecen a otros sectores que no son el tecnológico y también necesitan dotarse de sistemas seguros, grandes empresas de la automoción, pequeñas y medianas empresas de diferentes sectores, etc... Para estas empresas, a día de hoy, la seguridad no es su máxima preocupación, ya que su modelo de negocio tan sólo está empezando a extenderse a través de Internet. Es entonces cuando nos damos cuenta de que las grandes compañías tecnológicas están marcando el objetivo a alcanzar y el resto de compañías de otros sectores van en la misma dirección y es en esa dirección dónde la seguridad será aún más importante de lo que lo es hoy en día.

Cabe decir, que los objetivos de este proyecto no van enfocados a un trabajo de investigación de nuevas medidas de seguridad o de nuevas técnicas de ataques a sistemas, sino que están enfocados al estudio y el análisis de herramientas y técnicas ya existentes en la actualidad.

4 ESTRUCTURA DEL PROYECTO

El proyecto se ha dividido en módulos para facilitar la consecución y desarrollo de los objetivos. Cada uno de los módulos es tratado individualmente, aunque se nutren de información los unos de los otros.

En el módulo de diseño de la infraestructura de red, seguridad y detección de intrusiones se compone en primera instancia del diagrama de red de las sedes de la empresa. Como podemos ver en la figura 1 cada una de las sedes tiene alojados unos servicios en su Local Area Network (LAN). La sede nº 1 tiene alojado un servidor web y una base de datos, por otro lado, la sede nº 2 aloja un servidor de almacenamiento, bajo el protocolo File Transport protocol (FTP) y otra base de datos. Como podemos observar, en cada una de las puertas de entradas de las sedes hay un firewall inspeccionando y analizando el tráfico que entra y sale entre Internet y las sedes. Estos firewalls tienen la función de proteger la privacidad de los trabajadores e información de los sistemas que se alojan en las LAN's, además si en algún momento sufren un ataque son capaces de identificar los atacantes e incluso de minimizar el impacto que este causaría.

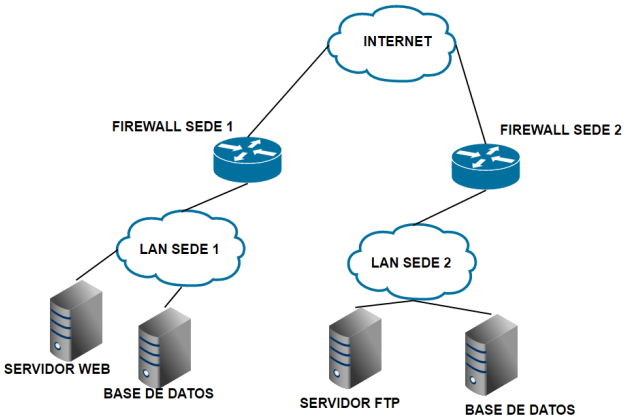

Fig. 1: Infraestructura de red de la empresa

El módulo de monitorización y análisis del rendimiento de los servicios y la red se nutre de la información que proporciona la red diseñada e implementada en el módulo anterior. Además, dado que los firewalls analizan y registran el trafico entrante y saliente, nos permite realizar análisis sobre el estado y el rendimiento, tanto de la red local como de los servicios alojados.

El último de los módulos en los que he dividido el proyecto, análisis de vulnerabilidades y explotación de las mismas, lo he dividido en dos secciones:

- La primera sección se refiere a las vulnerabilidades más comunes que pueden existir en un sistema. Como por ejemplo, ataques de fuerza bruta a servicios abiertos a Internet buscando el usuario y contraseña correctos, el escaneo de puertos que se puede considerar el paso previo a la realización de un ataque, la denegación de servicios, etc...
- En la segunda sección, se hace referencia a vulnerabilidades que podemos encontrar realizando un escaneo con herramientas específicas, en este caso se ha utilizado Nessus[1], a una máquina en concreto. En este caso se analizan las vulnerabilidades de los servicios y aplicaciones instalados.

5 METODOLOGIA

La metodología elegida para la realización de los objetivos de cada uno de los módulos de este proyecto es el modelo en espiral[2]. Esta metodología consiste en abordar los módulos del proyecto como si estos fueran ciclos o iteraciones que se repiten en forma de espiral, comenzando desde el centro.

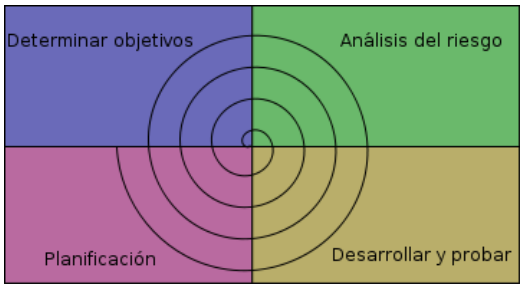

Fig. 2: Etapas del modelo de metodología en espiral

En la iteración de cada módulo hay que tener en cuenta:

- El objetivo: qué necesidad debe cubrir este módulo en el conjunto del proyecto.
- Las alternativas: las diferentes formas de lograr el correcto funcionamiento del módulo que se está iterando, dada la posibilidad de que la decisión inicial fuera incorrecta.
- El desarrollo y la verificación: Desarrollar y probar las funcionalidades implementadas. Si el resultado no es el adecuado o se necesitan implementar mejoras o nuevas funcionalidades, se planificarán las siguientes etapas y dará comienzo a un nuevo ciclo en la espiral:

    1. La determinación de los objetivos: En la primera iteración de la espiral, en esta etapa se definirán los objetivos iniciales, además se definirán los requisitos de la funcionalidad y las especificaciones, se fijarán las restricciones y se definirán las estrategias alternativas para evitar que los riesgos que entraña la realización del módulo no compliquen su consecución.
    2. El análisis de riesgos: Durante esta etapa se llevan a cabo estudios de posibles inconvenientes que impidieran el correcto desarrollo de la implementación. Se evalúan alternativas a los objetivos iniciales.
    3. El desarrollo y la realización de pruebas: En esta etapa se realiza el desarrollo de los objetivos establecidos en las etapas anteriores. Una vez finalizado el desarrollo o durante el mismo se realizan pruebas y comprobaciones. Al final de esta etapa se analizan las posibles alternativas a los escollos que se han ido encontrando durante el desarrollo.
    4. La planificación: Se trata ya de la última etapa de la iteración. Se recaba toda la información obtenida a lo largo de la iteración y se planifican los cambios y nuevos objetivos para la siguiente iteración.

6 DISEÑO DE LA INFRAESTRUCTURA DE RED, SEGURIDAD Y DETECCIÓN DE INTRUSIONES

6.1. Introducción

El diseño de la infraestructura de red de la empresa y sus sedes se ha realizado utilizando una herramienta online llamada Gliffy[3], en su versión de prueba, enfocada a la creación de diversos tipos de diagramas, entre ellos, los diagramas de red.

Una vez realizado el diseño inicial de la infraestructura, se ha utilizado una máquina virtual Debian 7.X de 32 bits para lanzar el simulador de redes Common Open Research Emulator[4] (CORE) y plasmar en él el diseño previamente realizado.

Cuando se finaliza el diseño de la infraestructura de red en el simulador CORE, se lanza la simulación. Llega entonces la hora de empezar a implementar la seguridad en los firewalls de ambas sedes utilizando iptables[5].

6.2. Iptables

Para realizar la implementación de los firewalls de las sedes de la empresa se ha utilizado la herramienta iptables, disponible en el núcleo de Linux. Iptables además de interceptar y manipular paquetes de red también permite realizar traducción de direcciones de red (NAT) o realizar registros de log. Para la realización del proyecto también se ha utilizado el módulo de sistema de seguimiento de conexiones (conntrack).

Iptables permite definir reglas acerca de qué decisión tomar con cada paquete de red. Estas reglas están agrupadas en cadenas, donde cada cadena contiene una lista ordenada de reglas; y además las cadenas se agrupan en tablas, donde cada tabla está asociada a un tipo diferente de procesamiento de paquetes.

Además, iptables permite crear nuevas tablas, también permite crear o eliminar cadenas, a excepción de las predeterminadas. Las tres tablas predeterminadas de las que se compone principalmente iptables son las siguientes:

- Tabla de filtrado: Es la encargada de denegar o permitir que un paquete pueda continuar hacía su destino. Predefinidamente contiene las cadenas INPUT, OUTPUT y FORWARD, cualquier paquete deberá pasar por una de ellas.
- Tabla de NAT: Tiene la función de realizar la reescritura de direcciones IP o puertos, tanto de origen como de destino, que contiene un paquete. Contiene las cadenas INPUT, OUTPUT, PREROUTING, POSTROUTING.
- Tabla mangle: Se encarga de modificar las opciones de cada paquete, todos los paquetes pasan por ella y contiene todas las posibles cadenas predefinidas, INPUT, OUTPUT, FORWARD, PREROUTING y POSTROUTING.

El administrador de redes, puede además, crear nuevas cadenas y asociarlas a una tabla. Como se ha dicho anteriormente, las cadenas contienen reglas. Cuando un paquete entra en el firewall pasa por cada una de las reglas, en el

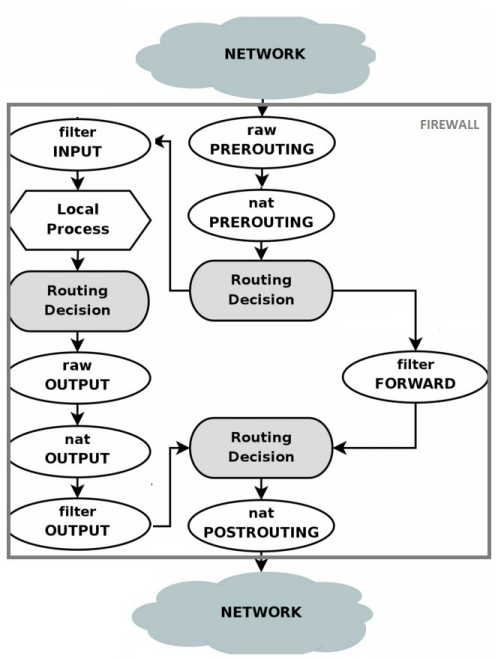

Fig. 3: Diagrama de decisiones de enrutamiento en iptables

orden en el que han sido introducidas, analizando si la cumplen. Las reglas analizan las propiedades del paquete y tanto si las cumple como si no, se les asigna un destino. Existen algunas restricciones y es que no todas las propiedades de los paquetes se pueden examinar en cualquier cadena, por ejemplo, la interfaz de red de salida no se puede analizar en la cadena INPUT.

En el párrafo anterior, se ha hablado sobre el destino de los paquetes al ser examinados por las reglas y es que un paquete puede tener como destino, otra cadena creada por el administrador de redes o los destinos ya predeterminados, ACCEPT, DROP, LOG, NAT de destino (DNAT) y NAT de origen (SNAT).

6.3. DNAT Y SNAT

Como se ha dicho anteriormente, la empresa en la que se ha basado el diseño de la estructura de red del proyecto tiene 2 sedes y cada una de ellas tiene alojados unos servicios, un servidor web y un servidor FTP respectivamente.

Cuando un usuario se intenta conectar a cualquiera de estos servicios, que están alojados detrás de los firewalls, debemos de asegurarnos de que la conexión ofrece la mínima información posible sobre la estructura de red interna, ya que el sistema debe parecer homogéneo y seguro.

Los usuarios no deben conectarse de forma directa a los servidores, como se ha dicho antes, deben pasar por los firewalls. Esto quiere decir, que una vez el usuario haya pasado la seguridad implementada en el firewall, se deberá redirigir su conexión al servicio que ha solicitado, lo que conlleva la utilización de DNAT, o lo que sería lo mismo, reescribir la dirección de destino de la conexión y poner la dirección interna del servidor.

Una vez realizada esta operación, todos los paquetes que el usuario y el servidor intercambien, pasarán a través del firewall y se les aplicará esta operación de reescritura en la dirección de destino, lo que quiere decir, que si el usuario analiza los paquetes que recibe del servidor, verá que la dirección de origen es diferente a la que él se conectó. De este modo podría deducir que se trata de la dirección interna del servidor y se estaría dando información sobre la red interna de la empresa.

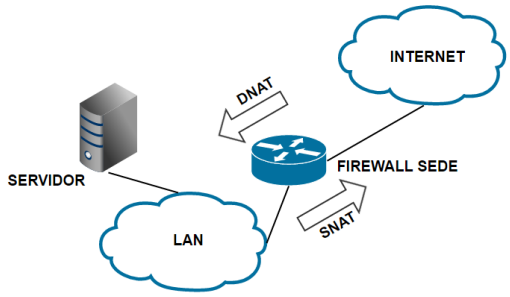

Fig. 4: Esquema del funcionamiento de SNAT y DNAT

Para evitar esta situación, se debe realizar SNAT desde el firewall desde el que se está analizando cada paquete del usuario, sustituyendo la dirección de origen, que será la dirección interna del servidor, por la dirección a la que el usuario se conectó para utilizar el servicio, creando así la sensación de homogeneidad y centralidad de la red.

6.4. VPN

A lo largo de una jornada laboral puede darse el caso de que deba compartirse información sensible entre sedes, dada la estructura de la red y la distancia física entre las sedes, esa información viajará por Internet pudiendo ser interceptada por terceras personas.

Una solución a este problema puede ser implementar una Virtual Private Network (VPN) entre ambas sedes. Esta VPN viene a ser una conexión directa ficticia entre dos puntos a través de un túnel, en este caso en particular, los firewalls de ambas sedes, dónde los paquetes y la información que transportan va encapsulada en la capa de protección que aplica la VPN.

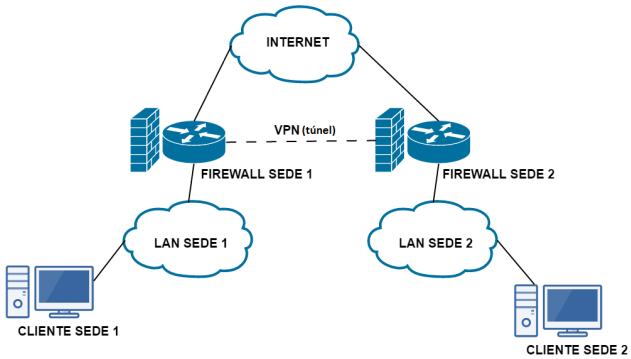

Fig. 5: Esquema de la VPN entre sedes de la empresa

Para que los paquetes puedan viajar a través de esta conexión segura, el firewall de la sede de origen del paquete, lo encapsula en un nuevo datagrama con su dirección del túnel como dirección origen y con la dirección del firewall de la otra sede del túnel como dirección destino. Así, cuando el otro firewall recibe el paquete, desencapsula el envoltorio que necesitaba para viajar por el túnel de la VPN y ya lo puede entregar a su destinatario en la red interna de la sede. Cabe recalcar que al encapsular el datagrama en el firewall

de la sede origen y desencapsularlo en el firewall de la sede destino, ha viajado cifrado y con direcciones diferentes a las originales, a través de Internet.

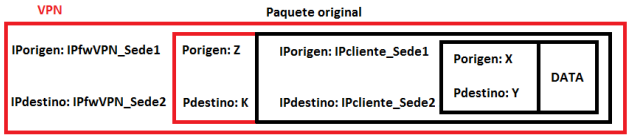

Fig. 6: Paquete enviado de un usuario a otro que ha sido encapsulado para poder viajar por la VPN

De este modo y gracias a la implementación de la VPN obtenemos privacidad sobre los datos y el anonimato en las direcciones en un entorno hostil como Internet.

6.5. DMZ

La Zona Desmilitarizada (DMZ) es una red, que se ubica entra la red interna y la red externa, generalmente Internet, de una empresa. Se trata de una red en la que normalmente se ubican los servidores que necesitan ser accedidos desde Internet y desde la que no se tiene acceso a la red interna. Esto implica que, si los servidores alojados en la DMZ fueran comprometidos por un agente externo, el problema no se extendería a la red interna y viceversa.

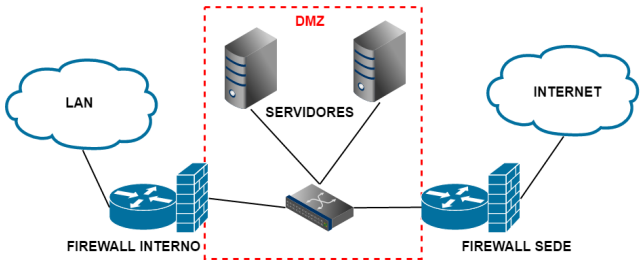

Fig. 7: Estructura de una DMZ

6.6. Port knocking

El concepto de port knocking vendría a ser el de pulsar una secuencia de botones en el orden correcto para poder acceder a través de una puerta a un sistema seguro, si la secuencia marcada no es correcta o se ha marcado en un orden diferente al preestablecido, la puerta no se abrirá.

En concreto cuando un usuario utiliza port knoking intenta realizar conexiones por determinados puertos, debiendo realizarse estas conexiones en el orden preestablecido. Si la secuencia es correcta, el firewall permite acceder a uno o varios puertos, en función de la configuración, que antes estaban cerrados. De esta manera se permite el acceso a un usuario acreditado a utilizar servicio solicitado, no sin antes utilizar las credenciales más clásicas, usuario y contraseña.

6.7. Logs

Como se ha comentado en un apartado anterior, los logs son unos registros que se guardan en un archivo de texto en el cuál se registran los paquetes que cumple alguna de las reglas que haya implementado el administrador de red.

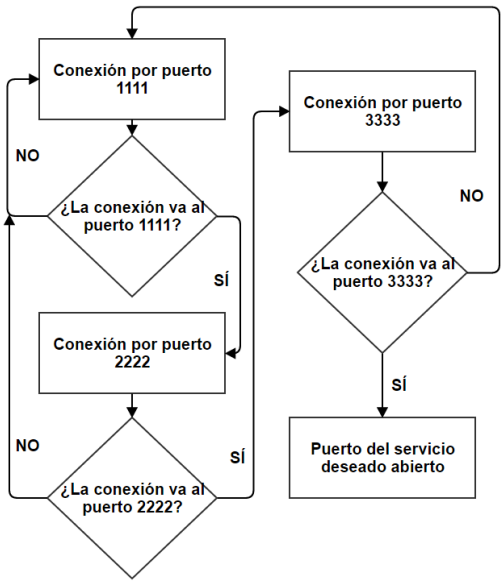

Fig. 8: Diagrama de flujo del port knocking

En estos registros aparece un mensaje que previamente ha especificado el administrador, la dirección de origen y de destino y demás información que puede ser útil para el administrador de red.

También se pueden utilizar a modo de detección de intrusiones, saber cuál es su origen y tomar medidas contra las direcciones de origen del ataque. Además, son pistas que deja un posible atacante, al cual se pueden estudiar sus movimientos y mejorar el sistema para futuros intentos.

7 Monitorización y análisis del rendimiento de los servicios y la red

7.1. Introducción

En la infraestructura de red de una empresa hay diferentes nodos y elementos interconectados por los que fluye información y datos. Existen la red interna de la empresa y la red externa de la empresa, que sería Internet y entre ellas también existe un flujo de datos con información que entra y sale de la empresa. Para anticiparse a posibles ataques y/o detectar una intrusión se debe monitorizar el tráfico de la red interna y su frontera, el firewall, ya que cualquier anomalía puede suponer el principio de un ataque. Además, alojados en la red interna tenemos alojados a los servidores de la empresa, los cuales suelen ser el blanco preferido de los intrusos, por lo que también se necesitará analizar y monitorizar sus recursos y rendimiento.

A lo largo del proyecto se han definido dos estados en los que se puede encontrar la red de la empresa, un estado normal, que es aquél que se repite a lo largo del tiempo con mayor frecuencia con pequeñas variaciones debido al número de máquinas activas y un estado de sobrecarga de la red, en el que se está realizando un mal uso de la misma, ya sea inconscientemente o de manera consciente siendo víctimas de un ataque. Debido a que la política de la empresa sólo permite a los trabajadores navegar por páginas webs, la mayor parte de la carga recae en los servidores, por lo tanto, este módulo estará mayoritariamente dedicado a ellos.

Para simular tráfico aleatorio en la red interna a lo largo

de una jornada laboral, se ha utilizado la herramienta Apache Benchmark v2.3[6], además, para generar los gráficos de éste módulo se ha utilizado la herramienta Webalizer[7], que utiliza los logs de acceso generados por apache para construir los gráficos que aparecerán a continuación.

Por otro lado, y de manera pasiva, se utiliza Snort v2.9.2.2[8] para examinar cada paquete entrante y saliente de la red interna a fin de detectar comportamientos sospechosos o peligrosos para la integridad del sistema.

7.2. Estado normal de la red

Cuando estipulamos que la carga de red es normal, se está diciendo que cumple un patrón ya conocido, ya que anteriormente y en la misma franja temporal se han repetido los mismos resultados.

En la figura 11 se muestra el gráfico con los accesos realizados al servidor web alojado en la sede 1 a lo largo de un día laborable. Se observa como a lo largo del día se ha mantenido un número de accesos constante, por lo que no se ha producido ninguna actividad sospechosa. También disponemos en la figura 10 el estado de los recursos del servidor web en un instante de tiempo puntual a lo largo del mismo día laborable. Debido a que los accesos al servidor se han mantenido en un número cercano a la normalidad, el servidor tampoco ha utilizado gran cantidad de sus recursos.

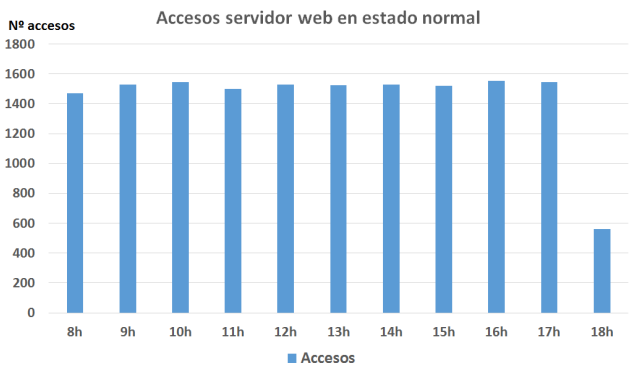

Fig. 9: Gráfico que muestra el número de accesos que se han realizado al servidor web entre las 8:00h y las 18:00h

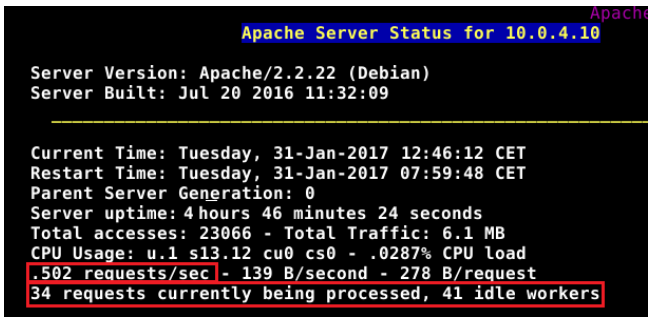

Fig. 10: Monitorización de los recursos en un estado de red normal

7.3. Estado sobrecargado de la red

Durante el episodio en el que se ha entrado en el estado de sobrecarga, se ha recibido un ataque desde la red externa al servidor web, en ese momento el firewall no tenía las reglas que reducen la efectividad de este tipo de ataque activadas a modo de demostración. Se puede observar en la figura 13, como durante la madrugada aumenta considerablemente el número de accesos respecto al estado normal de la red que apenas se aprecia en el gráfico. Además si se monitoriza el rendimiento del servidor, se puede observar que el rendimiento de la CPU no aumenta, pero sí el número de procesos que se están dedicando a servir el contenido solicitado.

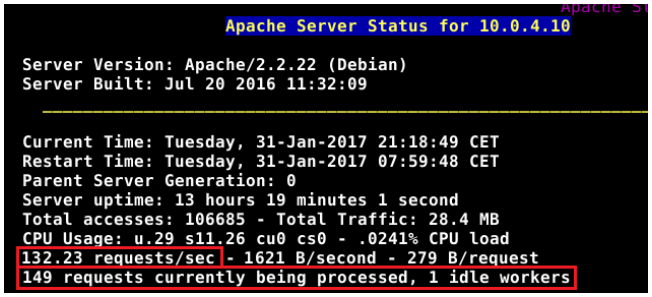

Fig. 11: Monitorización de los recursos en un estado de red sobrecargada

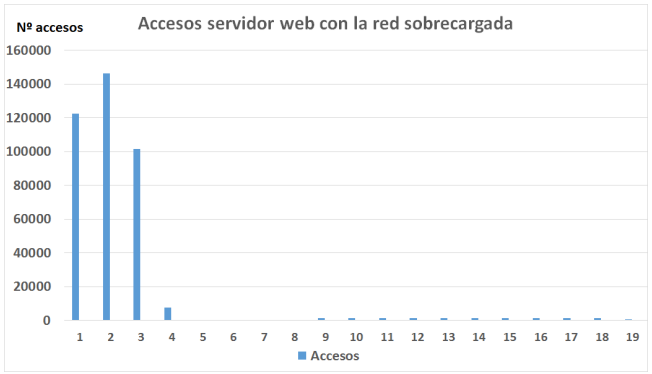

Fig. 12: Gráfico que muestra el número de accesos que se han realizado al servidor web entre la 1:00h y las 18:00h

7.4. Snort

Este software escanea permanentemente todos los paquetes y permite tomar contramedidas cuando alguna de las reglas establecidas previamente se cumple. UN ejemplo de su funcionamiento podría ser alertar al administrador de redes si se está buscando contenido no permitido en una web.

8 Análisis de vulnerabilidades y explotación de las mismas

8.1. Introducción

En este módulo se pasa a analizar las diferentes vulnerabilidades que se pueden encontrar en una infraestructura de red y sus servicios. Cuando parte de una infraestructura de red está disponible para la red externa y se ofrecen diferentes servicios, es importante tener actualizadas las versiones de los mismos, ya que periódicamente van apareciendo nuevas amenazas. Lo mismo ocurre con el hecho de la seguridad en los firewalls, la cual se debe ir manteniendo para

mantener la red segura ante la aparición de nuevas modalidades de ataques y el aumento de la complejidad de los mismos.

8.2. Vulnerabilidades en el sistema

8.2.1. Escaneo de puertos

El escaneo de puertos realiza una búsqueda en una máquina previamente indicada de los puertos que están abiertos. El resultado de esta acción es una lista del estado de los puertos analizados por la herramienta elegida para llevarlo a cabo.

La acción de realizar un escaneo de puertos no se entiende como un ataque en si mismo, ya que en ningún momento se intenta penetrar la seguridad del sistema o dejarlo fuera de servicio, simplemente se trata de la obtención de información de la maquina deseada. No obstante, se trata del paso previo a la realización de un ataque ya que, generalmente, detrás de un puerto abierto hay un servicio esperando peticiones.

En los firewalls que se han implementado en el proyecto, no se permiten los escaneos de puertos, para así dificultar el éxito de un ataque. Para evitar esta acción, se ha creado una regla que indica que sí se intenta acceder por un puerto en concreto, que generalmente, está en desuso, se interpreta como que la máquina que ha realizado dicho intento está realizando un escaneo de puertos. La medida que se aplica una vez se cumple la regla, es la de bloquear la dirección de la máquina que ha realizado el escaneo durante 24h.

8.2.2. Ataques de denegación de servicio

En el apartado en el que el estado la red estaba sobrecargado se ha recibido un ataque de denegación de servicio que ha provocado que los usuarios que pretendían realizar un buen uso del servidor, les fuera imposible, ya que el servidor, o estaba atendiendo a las peticiones maliciosas o para proteger su integridad, el sistema decidió dejar de escuchar más peticiones y poder así recuperarse de la sobrecarga.

Para proteger a los servidores de la empresa de este tipo de ataques se han implementado una serie de reglas en iptables que limitan el número de accesos por dirección, cuando se sobrepasa el umbral establecido como máximo, la dirección queda automáticamente excluida y ya ni siquiera, aún que vuelva a un número de accesos por debajo del umbral se le atenderá. Está decisión de bloquear las direcciones que sobrepasan el umbral se ha tomado porque, si únicamente se establecía un número de accesos por segundo, el firewall debía de estar constantemente calculando el umbral y provocaba que el servicio no funcionara tal y como debería.

8.2.3. Ataques de validación de credenciales por fuerza bruta

Los ataques de validación de credenciales por fuerza bruta tienen el cometido de lograr adivinar las credenciales de algún usuario, preferiblemente súper usuario, para utilizar cualquier servicio para el que su acceso esté disponible para la red externa. La realización del ataque pasa por realizar numerosos intentos probando diferentes usuarios y contraseñas hasta dar con alguna pareja que sea correcta. Normalmente, para la realización de este tipo de ataques se utilizan un archivo con nombres de usuario utilizados comúnmente y otro archivo de contraseñas generadas a partir de unos parámetros configurables.

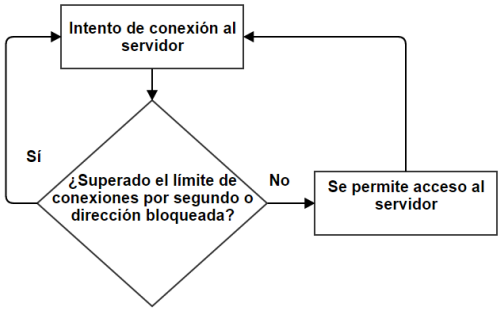

Fig. 13: Diagrama de flujo de las reglas implementadas para evitar los ataques de denegación de servicio

Una medida para contrarrestar este tipo de ataques es el mismo que hemos aplicado en el apartado anterior, limitar el número de intentos que el atacante pueda realizar contra el servicio, de este modo el tiempo que el atacante tardará en obtener las credenciales válidas crecerá considerablemente, ya que por muchos recursos de los que disponga el atacante, estará limitado por la regla del firewall que bloqueará sus intentos.

8.3. Vulnerabilidades en las aplicaciones del sistema

Para la búsqueda de vulnerabilidades en los diferentes servicios instalados en un servidor, utilizaremos una herramienta conocida como Nessus, que escanea, analiza y ordena por peligrosidad las vulnerabilidades que encuentra en las aplicaciones de un sistema.

Nessus utiliza para identificar cada vulnerabilidad el sistema de Common Vulnerabilities and Exposures (CVE)[9], que es una lista de información registrada sobre vulnerabilidades conocidas que fue definida y es mantenida por Mitre Coportation. En esta lista cada referencia tiene un número de identificación único, el formato para cada entrada CVE es: CVE-YYYY-NNNN, donde YYYY indica el año y NNNN el número de vulnerabilidad. Además de identificar cada vulnerabilidad de manera única, se le asigna el impacto que tiene sobre el sistema utilizando un sistema de puntos, Common Vulnerability Scoring System v3 (CVSS)[10], en el que a cada vulnerabilidad se le asigna una puntuación en función de su peligrosidad.

9 Resultados

En esta sección del proyecto se pondrá en práctica las técnicas y contextos de los que se ha hablado a lo largo del artículo. Esta serie de pruebas se dividirán en tres grupos, que corresponden a los módulos en los que se ha dividido el proyecto.

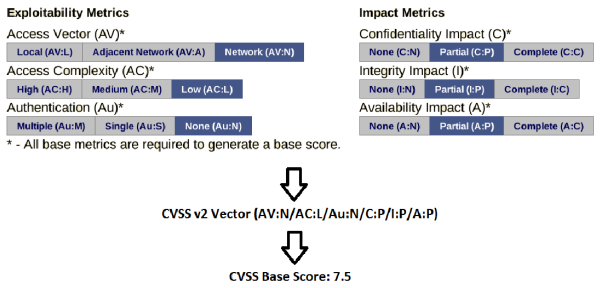

Fig. 14: Métricas utilizadas por CVSS para generar el vector de la vulnerabilidad y su puntuación

9.1. Diseño de la infraestructura de red, seguridad y detección de intrusiones

9.1.1. Ataques de denegación de servicio

En la sección de resultados respecto a los ataques de denegación de servicio se va a realizar una comparación de la disponibilidad del servidor web que tienen los usuarios en ambos casos, sin la seguridad necesaria implementada en el firewall y con la seguridad implementada. Se va a proceder a lanzar un ataque para inundar de peticiones el servicio web de la empresa. Para realizar este ataque se utilizará la herramienta nping y se ejecutará el siguiente comando: nping –tcp-connect -rate=90000 -c 900000 -q [dirección], el cual intentará lanzar 90000 conexiones por segundo durante 900000 ciclos contra la dirección del servidor web. El propósito de este ataque es sobrecargar de peticiones el servidor web y dejar sin acceso a los usuarios que intentan realizar un correcto uso del sistema.

Como podemos observar en la figura 16, cuando en el firewall no se aplica la seguridad necesaria contra este tipo de ataques se envían una cantidad de paquetes por segundo fuera de lo normal, de los cuáles, el servidor debido a los recursos de los que dispone, tan solo puede responder a un 6 % de las peticiones que se han realizado, dejando ver que está sobrecargado y no puede atender apenas peticiones ya que no dispone de los recursos suficientes para ello. Además, se ha realizado un intento de conexión desde otra máquina diferente al atacante y ha sido imposible obtener respuesta por parte del servidor.

	Conexiones				
Tiempo: 10s	*Intentos*	*Satisfactorias*	*Fallidas*	*Pkts enviados/s*	*Pkts recibidos/s*
Sin seguridad	36998	2197	34801	3755	223
Con seguridad	41664	3	41661	3567	0.26

Fig. 15: Tabla con datos comparativos tras un ataque de denegación de servicio

Por otro lado, cuando se ha aplicado la seguridad necesaria al firewall. Se observa como ha detectado al atacante y ni siquiera se le ha atendido al 1 % de las peticiones que ha realizado. En este caso, mientras el ataque estaba en curso, se ha realizado una conexión al servidor web con otra máquina que no era la atacante y no ha habido ningún problema de disponibilidad del servidor.

9.1.2. VPN

En referencia a la VPN instalada entre las dos sedes de la empresa, se puede observar en la figura 7, como los paquetes interceptados que viajan por Internet, están encapsulados en otros paquetes dónde la información que aparece, demuestra que está se han encaminado a través del túnel que utiliza la VPN. Esta información que aparece en los paquetes interceptados y que demuestran que se están enviando a través de la VPN, son los puertos de origen y destino del paquete, ya que son los que predeterminadamente utiliza la herramienta Openvpn[11]. Además, se observa como las direcciones de origen y destino son las que se utilizan como extremos de la red virtual.

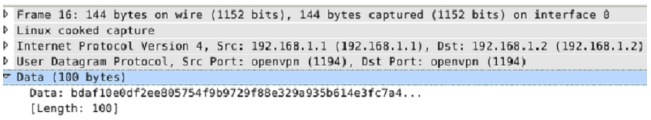

Fig. 16: Paquete interceptado en Internet perteneciente a la comunicación entre dos usuarios de la VPN

9.2. Monitorización y análisis del rendimiento de los servicios y la red

9.2.1. Alertas de búsquedas de contenido prohibidas

En la empresa hay ciertas normas en cuanto al contenido que está permitido buscar en Internet, para gestionar y controlar que está regla se cumple se ha implementado Snort para inspeccionar el contenido de cada paquete entrante y saliente de la red interna. Cuando alguien en la red interna incumple esta directiva, al administrador de redes le aparece una alerta como la podemos ver en la figura 18, conforme se ha buscado en Internet algún contenido restringido y la dirección de la persona que lo ha hecho. En esta imagen en concreto, un usuario de la red interna ha realizado la búsqueda de términos prohibidos como, Facebook y games.

```
[**] [1:10050:0] Games content found [**]
[Priority: 0]
02/04-00:24:27.518487 192.168.24.132:47556 -> 216.58.201.131:80
TCP TTL:64 TOS:0x0 ID:13198 IpLen:20 DgmLen:583 DF
***AP*** Seq: 0x96982677  Ack: 0x4F066C60  Win: 0x7210  TcpLen: 20

[**] [1:10050:0] Facebook content found [**]
[Priority: 0]
02/04-00:26:53.867888 192.168.24.132:47578 -> 216.58.201.131:80
TCP TTL:64 TOS:0x0 ID:55148 IpLen:20 DgmLen:588 DF
***AP*** Seq: 0x6BB3738D  Ack: 0x37B629B8  Win: 0x7210  TcpLen: 20
```

Fig. 17: Alertas recibidas por el administrador cuando un usuario realiza búsquedas no permitidas en Internet

9.2.2. Logs para monitorizar el tráfico de la red interna

Los logs puede tener múltiples utilidades, pero en este proyecto se han utilizado para monitorizar el flujo de datos que entra y sale de la red interna. Se monitoriza quién y cuántas veces sale a Internet, quién y cuántas veces se conecta a algún servicio de la red interna, quién y cuando está intentando realizar un escaneo de puertos, los accesos e intentos de accesos por ssh utilizando port knocking, etc...

En la figura 19 se muestran algunos ejemplos de estos logs y del formato que tienen.

```
'9701] LAN-INTERNET: IN=eth0 OUT=eth2 MAC=00:00:00:aa:(
:0693] LAN-INTERNET: IN=eth0 OUT=eth2 MAC=00:00:00:aa:(
'9485] INTERNET-LAN: IN=eth2 OUT=eth0 MAC=00:00:00:aa:(
:0894] INTERNET-LAN: IN=eth2 OUT=eth0 MAC=00:00:00:aa:(
)] PORTSCAN: IN=eth2 OUT= MAC=00:00:00:aa:00:06:00:0(
:0047] HTTP-IN: IN=eth2 OUT=eth0 MAC=00:00:00:aa:00:06
:0116] HTTP-OUT: IN=eth0 OUT=eth2 MAC=00:00:00:aa:00:0(
:2226] Knock accepted: IN=eth1 OUT= MAC=00:00:00:aa:00
:2386] Knock accepted: IN=eth1 OUT= MAC=00:00:00:aa:00
:2810] Knock accepted: IN=eth1 OUT= MAC=00:00:00:aa:00
:6786] Knock accepted: IN=eth1 OUT= MAC=00:00:00:aa:00
:9353] Knock accepted: IN=eth1 OUT= MAC=00:00:00:aa:00
```

Fig. 18: Logs generados a partir de los paquetes entrantes y salientes de la red interna

9.3. Vulnerabilidades en el sistema

9.3.1. Ataque de validación de credenciales por fuerza bruta en Tomcat

En este ataque el objetivo es explotar una vulnerabilidad en la aplicación Tomcat instalada en una máquina objetivo. Dadas las características de la vulnerabilidad y tras haber realizado un escaneo con la herramienta Nessus en la máquina objetivo, el reporte ha arrojado que el servidor web Tomcat que tiene instalado puede tener aún las credenciales de acceso remoto predeterminadas. Esta vulnerabilidad está identificada con la id CVE-2010-4094[12].

Para intentar conseguir las credenciales de acceso al servidor web Tomcat objetivo, se utilizará la herramienta Hydra para lanzar el ataque de fuerza bruta, que a su vez utilizará un archivo con posibles nombres de usuario y contraseñas. Para comprobar la efectividad de este ataque se van a realizar dos intentos, uno con la seguridad contra los ataques de fuerza bruta que utiliza el mismo principio que la seguridad contra los ataques de denegación de servicio, activada y otro intento sin esta seguridad activa.

En la figura 20 se puede ver como sin la seguridad adecuada, se ha podido conseguir la contraseña y usuario para acceder a la consola de administración de la aplicación Tomcat.

```
[ATTEMPT] target 192.168.24.131 - login "tomcat" - pass "tomaot" - 8668 of 15625
 [child 2]
[8180][http-get] host: 192.168.24.131   login: tomcat   password: tomcat
[STATUS] attack finished for 192.168.24.131 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

Fig. 19: Resultado obtenido al realizar un ataque de fuerza bruta sobre un servidor web Tomcat sin seguridad implementada

Por otro lado, con la seguridad implementada, en la figura 21 la herramienta Hydra ha lanzado un mensaje avisando de que la comprobación de todas las posibles combinaciones de credenciales, según sus estimaciones, va a llevar alrededor de 8h. Cabe decir que para ambos intentos se han utilizado los mismos parámetros y ficheros de usuarios y contraseñas.

9.3.2. Ataque al servicio vsftpd v2.3.4

Durante el escaneo de Nessus en el ataque anterior, se ha podido observar como el servicio vsftpd v2.3.4 instalado en

```
[ATTEMPT] target 192.168.24.131 - login "tomcat" - pass "cccaat" - 33 of 15636
child 2]
[STATUS] 33.00 tries/min, 33 tries in 00:01h, 15592 to do in 07:53h, 16 active
[VERBOSE] Retrying connection for child 0
[VERBOSE] Retrying connection for child 4
```

Fig. 20: Resultado obtenido al realizar un ataque de fuerza bruta sobre un servidor web Tomcat con seguridad implementada

la máquina objetivo contiene una vulnerabilidad en la que añadiendo una cara sonriente al nombre de usuario con el que intentamos validar las credenciales, se abre una puerta trasera con permisos de súper usuario. Esta vulnerabilidad tiene la id CVE-2011-2523[13].

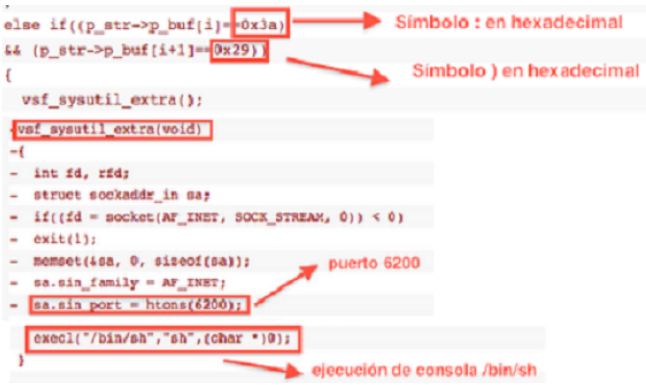

Fig. 21: Vulnerabilidad en el código fuente del servicio vsftpd v2.3.4

En la figura 23 se puede observar que se ha logrado el objetivo del ataque. Para evitar este tipo de ataque es conveniente mantenerse informado sobre las noticias que acontecen a los servicios que se tienen instalados y actualizarlos cuando es debido.

```
root@kali:~# ftp 192.168.24.131
Connected to 192.168.24.131.
220 (vsFTPd 2.3.4)
Name (192.168.24.131:root): root:)
331 Please specify the password.
Password:
root@kali:~# netcat 192.168.24.131 6200
whoami
root
```

Fig. 22: Resultado obtenido tras realizar el ataque contra el servidor FTP

9.3.3. Escaneo de puertos

Como se ha dicho con anterioridad, el escaneo de puertos no es un ataque en sí mismo, pero es considerado el paso previo a la realización de uno. Para que este tipo de prácticas no consigan su propósito que es el de visualizar los puertos abiertos que hay en los firewalls se ha aplicado una regla que banea, durante un tiempo, la dirección de la máquina que intente realizar dicha comprobación. De esta manera se provoca que el atacante no obtenga la información que pretendía. Para realizar el escaneo de puertos se ha utilizado la herramienta nmap y el comando: nmap -Pn [dirección].

Se puede observar en la figura 24, que el tiempo restante de ejecución no deja de aumentar a medida que pasa el

tiempo, ya que cada vez que intenta realizar el escaneo de puertos, la dirección es bloqueada. Por otro lado, si la seguridad respecto al escaneo de puertos estuviera desactivada, la herramienta nmap tarda apenas un segundo en devolver todos los puertos abiertos del firewall.

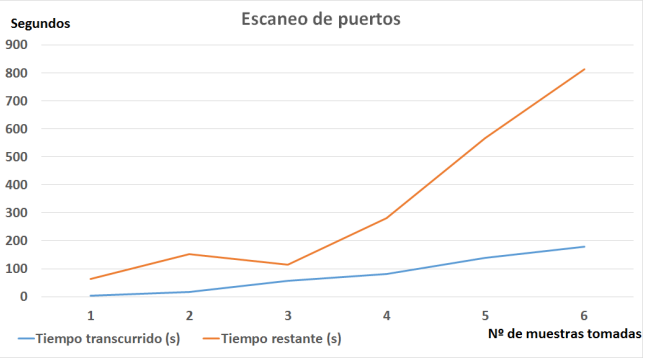

Fig. 23: Gráfico que muestra el tiempo estimado y transcurrido para terminar el escaneo de puertos de la máquina objetivo

10 Conclusiones

A lo largo del desarrollo del proyecto y de la elaboración de este informe se ha podido observar uno de los muchos diseños que puede tener la infraestructura de red de una empresa y los elementos que puede contener. También se ha mostrado las diferentes capas de seguridad que puede tener la empresa y lo importantes que son para ofrecer una total disponibilidad a los servidores de los que dispone. Además se ha mostrado la importancia de tener actualizados, monitorizados y de añadir seguridad extra todos los servicios que se utilizan, ya que por si mismos son vulnerables.

A lo largo de la realización del proyecto han ido surgiendo problemas de compatibilidades con los entornos de simulación y las interfaces de algunas herramientas, incluso algunos de los objetivos que se marcaron de inicio no se han llevado a cabo y se han intercambiado con otros que han ido surgiendo a lo largo del proyecto. La implementación de VLAN's se fue descartando a medida que iba avanzando el proyecto, ya que surgió la idea de utilizar una VPN y puesto que los dos objetivos no daría tiempo a cumplirlos se optó por el que pareció más práctico. Tampoco se han llevado a cabo los objetivos de backups en red ni los de balanceo de carga de los servicios internos debido a que el proyecto no ha girado entorno al contenido de los servidores y/o máquinas, sino su disponibilidad y accesibilidad, en cambio, se ha implementado la funcionalidad de port knocking.

Personalmente ha resultado ser una experiencia muy gratificante y enriquecedora ya que he podido plasmar el conocimiento obtenido, tanto en el grado, como en la realización del proyecto y he visto como el proyecto avanzaba y tomaba forma. Este proyecto me ha enseñado a trabajar de una manera más organizada y metódica utilizando los conceptos de la metodología en espiral.

10.1. Líneas futuras

Como se ha dicho en el apartado de conclusiones, algunos de los objetivos no se han alcanzado por falta de tiempo, ya que a medida que avanzaba el proyecto se intercambiaban por otros a priori más prácticos. No obstante, los objetivos principales no han quedado ni mucho menos descartados y harían mucho más completa la seguridad e integridad de la infraestructura de red de la empresa.

Por otro lado, ya en los últimos compases del proyecto han ido surgiendo ideas que ya no daría tiempo de implementar, por ejemplo, el software Snort, además de ofrecer un modo de detección y de control del tráfico de la red, tiene también la funcionalidad de protección y actuación frente diferentes situaciones que sería interesante implementar en un futuro.

10.2. Agradecimientos

Agradezco a mi tutor Juan Carlos, por haberme elegido para llevar a cabo el desarrollo del proyecto y por el apoyo proporcionado para llevarlo acabo.

Referencias

[1] Nessus, *https://www.tenable.com/products/nessus-vulnerability-scanner* [Consulta: 2 de Enero de 2017]

[2] Metodología en espiral, *http://modeloespiral.blogspot.com.es/* [Consulta: 28 de Diciembre de 2016]

[3] Gliffy, *https://www.gliffy.com/* [Consulta: 14 de Octubre de 2016]

[4] Common Open Research Emulator (CORE), *https://www.nrl.navy.mil/itd/ncs/products/core* [Consulta: 30 de Octubre de 2016]

[5] Netfilter (iptables), *https://www.netfilter.org/documentation/HOWTO/es/packet-filtering-HOWTO-7.html* [Consulta: 3 de Noviembre de 2016]

[6] Apache benchmark, *https://httpd.apache.org/docs/2.4/programs/ab.html* [Consulta: 5 de Enero de 2017]

[7] Webalizer, *http://www.webalizer.org/* [Consulta: 17 de Enero de 2017]

[8] Snort, *https://www.snort.org/* [Consulta: 4 de Enero de 2017]

[9] Common Vulnerabilities and Exposures, *https://cve.mitre.org/* [Consulta: 1 de Febrero de 2017]

[10] Common Vulnerability Scoring System, *https://www.first.org/cvss* [Consulta: 28 de Enero de 2017]

[11] Openvpn, *https://openvpn.net/ [Consulta: 11 de Enero de 2017]*

[12] CVE-2010-4094, *https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4094*