Estudio de Seguridades en la Nube

Frank Nazareno Montiel, Joanna Guevara Andrade, Giuseppe Blacio
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
frannaza@espolo.edu.ec, johi1709@gmail.com, gblacio@espol.edu.ec

Resumen

En este proyecto presentamos un conjunto de pruebas de seguridad de redes para el popular servicio de almacenamiento de datos en la nube DROPBOX, que se muestran como un complemento a las clases impartidas en las carreras de ingeniería y licenciatura relacionadas con las tecnologías de la información. En estas pruebas usamos la versión más actual del sistema operativo KALI LINUX el cual se virtualiza en una laptop, esto nos proporciona flexibilidad de hardware lo cual hace más eficaz nuestro estudio de seguridades en la nube , esto nos sirve para entender las medidas de seguridad teniendo como objetivo comprobar la integridad y confidencialidad de los datos del servicio nombrado anteriormente entre los dispositivos finales y su nube de almacenamiento, las herramientas utilizadas para recolectar y reconocer las posibles vulnerabilidades de este servicio considerado "Seguro. El documento está dividido secciones en el primero se presenta una teoría acerca de los servicios en la nube , en las siguientes secciones está dirigido a la seguridad, términos y conceptos de seguridad así como también los tipos de ataques, en el que sigue se detalla la arquitectura de la computación en la nube, finalmente en la última sección son las pruebas de penetración donde mostramos las pruebas que se realizan , y finalmente presentamos los resultados conclusiones y recomendaciones fundamentados en las nuestras pruebas.

Palabras Claves: *Nube, Dropbox, Kali Linx, conceptos de seguridad, pruebas de penetración*

Abstract

In this project we present a set of network security testing for popular data storage service in the cloud DROPBOX, shown as a complement to classes taught in undergraduate engineering programs and related information technologies. In these tests we used the latest version of KALI LINUX operating system which is virtualized on a laptop, this gives us the flexibility of hardware which makes our study more effective securities in the cloud, this helps us understand the security measures having intended to check the integrity and confidentiality of the above named service data between end devices and cloud storage, the tools used to collect and recognize the potential vulnerabilities of this service considered " sure. The document is divided sections in the first theory about the services presented in the cloud, in the following sections is aimed at security, terms and security concepts as well as the types of attacks, which follow detailed the architecture of cloud computing, and finally in the last section are penetration testing where we show the tests performed, and finally present the results conclusions and recommendations that build on our tests.

Keywords: *Cloud, Dropbox, Kali Linux, security concepts, penetration testing*

1. Introducción

El modelo de servicio de la computación en la Nube no necesariamente es una nueva tecnología más bien se pude decir que es una nueva forma de acceder a los recursos de computación. Además el termino Nube no es tan nuevo para los profesionales de TI, porque para representar una de red que no estábamos interesados en conocer su infraestructura en su totalidad sino solo saber que existen utilizábamos una nube para representarla.

Desde la invención de primera computadora siempre hubo la necesidad de obtener los mejores recursos informáticos para todos, pero en esos inicios era totalmente imposible con tecnologías tan caras. Pero posteriormente las maquinas abaratan su costo, pero eran equipos básicos en lo que respecta a su funcionamiento. Para mayores y más complicadas operaciones se utilizaban maquinas más potentes los conocidos *mainframes* maquinas potentes, grandes y costosas, en los que se distribuía el sistema.

Poco a poco los computadores personales fueron superando su capacidad y potencia y poco después interconectados en la gran red de redes. Internet. Ahora los usuarios podían generar información en la denominada Web 2.0.

2. Computación en la Nube

La Computación en la Nube (del inglés, *Cloud Computing*), también es conocido bajo los términos servicios en la Nube, informática en la Nube, es un modelo de negocio en que las tecnologías de información TI pueden ser ofrecidas como un servicio a través de la rede Internet.

La Computación en la Nube son servidores alojados en internet encargados de atender las peticiones de cualquier usuario en cualquier momento. Para tener acceso a este servicio, es necesario tener una conexión a Internet desde cualquier dispositivo móvil o fijo ubicado en cualquier lugar. Esta norma hace posible ahorro de costos y un mejor tiempo de actividad. [1]

Figura 1 Actividades en la Nube [1]

En la Nube Informática cada vez más se aumentan los servicios que ofrece a sus clientes. Esto resulta beneficioso para los usuarios que poseen más variedad para cubrir sus necesidades, de forma rápida y eficiente. Y ahorrando gasto económico en infraestructura TI y personal especializado. Y para una muestra la siguiente figura nos muestra las distintas actividades y servicios que disponen los consumidores de este servicio.

3. Tipos de niveles de servicios

Entre ellos son:

Infraestructura como servicio (IaaS)

Plataforma como servicio (PaaS)

Software como servicio (SaaS)

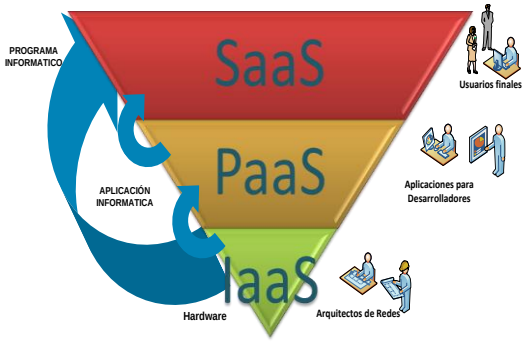

Figura 2 Niveles de Servicio [2]

3.1 Infraestructura como servicio (IaaS):

Infraestructura como servicio (IaaS, del inglés, Infraestructure as a Service) permite que los servidores sean creados en un entorno informático virtualizado sin las mismas restricciones que el hardware físico impone.

3.2 Plataforma como servicio (PaaS):

Son proveedores que se especializan en la reacción de entornos con propósitos específicos donde desarrolladores pueden subir su código sin tener que tomar en consideración los sistemas operativos, uso de recursos, etc.

3.3 Software como servicio (SaaS):

Son proveedores que ofrecen aplicaciones directamente a los usuarios finales y desarrollan en entornos proporcionados por las capas de IaaS y PaaS. SaaS tiene muchas ventajas para los usuarios finales, como modalidad de pago según los modelos, un desarrollo de software constante con la disponibilidad inmediata de nuevas versiones, menores costos de mantenimiento para usuarios y mucho más.

4. Modelos de Despliegue de Servicios

Nube Pública

Nube Híbrida:

Nubes Privadas

Nube Comunitaria

4.3 Nubes Privadas

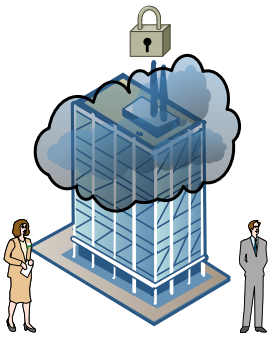

Figura 3 Nube Privada

En las Nubes privadas la administración de los procesos son internos y realizados por una única entidad que decide donde y como se ejecutan. Es de mayor seguridad y privacidad de los datos y procesos, porque la información sensible permanecerá dentro del proveedor. Aunque este se encargara de comprar, mantener y administrar la infraestructura tanto de hardware como de software.

4.5 Nube Pública

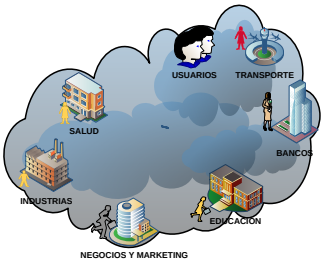

Figura4 Nube Pública

Las Nubes públicas son aquellas gestionadas por terceras personas para el control de los recursos, procesos y datos. En este modelo de despliegue, múltiples usuarios pueden hacer uso de los servicios de la Nube en un mismo servidor, compartiendo espacio en disco, infraestructura de red, etc. de manera transparente y segura a cada usuario.

4.1 Nube Híbrida

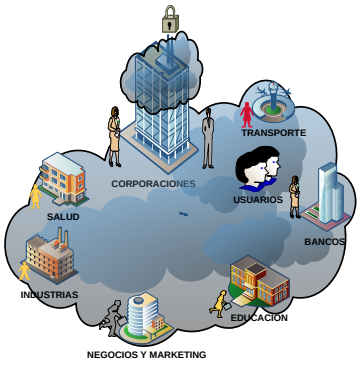

Figura 1 Nube Hibrida

Las Nubes hibridas combinan los 2 modelos anteriores, es decir coexisten ambos modelos la Nube Publica y la Nube privada. Es de mucha utilidad en la empresas por su flexibilidad para ilustrarlo supongamos que cierta empresa tiene un servidor web y para eso hace uso de la nube publica y para un servidor de base de datos hace uso de una Nube privada. De tal forma que la información sensible permanezca bajo estricto control local y mientras que la información del servidor web será administrada por un tercero en este caso el proveedor de Nube pública. Esto genera menor complejidad y ahorro en el costo de uso de la Nube privada

4.2 Nube Comunitaria

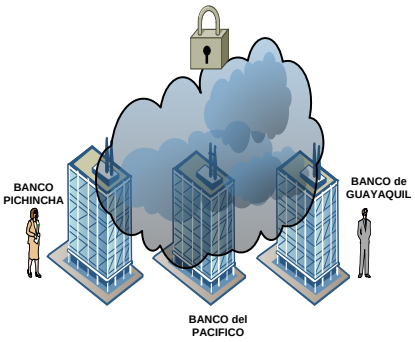

Figura 7 Nube Hibrida

Además de los 3 modelos anteriores se menciona uno más las nubes comunitarias, que son infraestructuras compartidas entre varias organizaciones que comparten un mismo fin, metas o requerimientos. Se podría decir que es como una variante de una nube privada

6. ANÁLISIS DE RIESGOS EN LA COMPUTACION EN LA NUBE

"La computación en Nube es un nuevo modo de facilitar recursos de computación, no una nueva tecnología. Ahora los servicios de computación, desde el almacenamiento y procesamiento de datos hasta el software, como la gestión del correo electrónico, están disponibles de forma instantánea, sin compromiso y bajo demanda […]. Desde el punto de vista de la seguridad, las economías de escala y flexibilidad en Nube son elementos tanto favorables como perjudiciales. Las concentraciones masivas de recursos y de datos constituyen un objetivo más atractivo para los atacantes, pero las defensas basadas en la Nube pueden ser más robustas, escalables y rentables."

7. ¿De qué nos queremos proteger? De todo aquello que pueda afectar los recursos del sistema que pueden ser:

- Personas: empleados, ex-empleados, curiosos, piratas, terroristas, intrusos remunerados
- Amenazas lógicas: que podrían ser software defectuoso, puertas traseras, virus, caballos de Troya, etc.
- Catástrofes naturales básicamente fuego, agua, derrumbes y

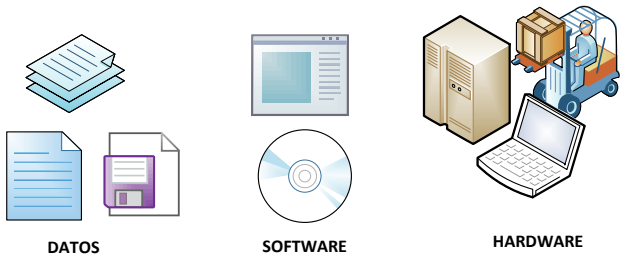

Figura 8 Recursos del sistema [3]

8 Principales Amenazas

En vista de la situación la *CSA Cloud Security Alliance* (por sus siglas en inglés, La alianza para la seguridad en la nube), regularmente publica informes técnicos sobre la principales vulnerabilidades a nivel mundial y para nuestro análisis veremos las principales amenazas a la Nube en el año 2013, publicado en Febrero 2013, es decir los informes más actuales con los que disponen.

Las nueve amenazas críticas se nombraran cada uno por orden de gravedad:

Principales Amenazas a la Nube		
	Orden de gravedad	Amenazas
2013	1	Filtraciones en los datos
	2	Pérdida de datos
	3	Secuestro de Cuentas o Tráfico
	4	Interfaces Inseguras e Interfaz de programación de aplicación
	5	Denegación de servicio
	6	Empleados maliciosos
	7	Abusos de servicios en la Nube

Tabla 1 Ranking de Amenazas [4]

9. Pruebas de Penetración

La implementación de esta prueba de penetración se realizara con el sistema operativo de prueba de penetración *KALI LINUX* esta distribución es proporcionada por los mismos creadores de *BACKTRACK* su antecesor, con la cual se realizara diversas pruebas donde podamos obtener datos que podamos estudiar para establecer amenazas y vulnerabilidades comprobada de estos sistemas en la Nube, y por falta de espacio nos limitaremos a mencionar las más importante, no sin antes describir las herramientas utilizadas,

.

10. Datos obtenidos del servicio web configurado por Dropbox (Herramienta WINHTTP)

Mediante la herramienta *winhttp* y en combinación con el NMAP obtuvimos información acerca del servicio web por decirlo así que es el método de conexión para compartir archivos, esto en el modelo cliente – servidor. El comando nmap -T4 -A -v www.dropbox.com nos arroja información acerca de los puertos abiertos, en TCP/IP los puertos entre TCP y UDP son 65535 luego del escaneo al dominio objetivo se obtuvo que todos los puertos se encontraban cerrados como medida de seguridad los únicos puertos abiertos son:

80 que es HTTP – TCP o (web)

443 que es HTTPS – TCP o (web-seguro), usado por páginas de bancos y sitios de transacciones monetarias.

En la gráfica también se muestra que existe un HTTPS METHOD que se traduce como una redirección automática del puerto 80 abierto al 443 abierto, es decir si uno abre una página web en un navegador cualquiera con www.dropbox.com automáticamente se abrirá el siguiente URL https://www.dropbox.com.

Es decir aunque el puerto 80 este abierto este no será usado ya que existe una redirección de http-https configurada en el servidor WEB, adicional a esto se pudo obtener información del certificado digital usado en dicho servidor WEB certificado emitido FQDN:

Commonname=*.dropbox.com

Organizationname=Dropbox, INC

Statename=California

Countryname=US

El certificado digital usa claves de tipo RSA. RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública. La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del orden de 10 elevado a la 200.[5]

La clave encontrada es una RSA de 2048 bits valido no antes de 2011-12-01 y no valido después de 2014-01-29, es decir este será renovado antes de esta fecha de caducidad como método de seguridad.

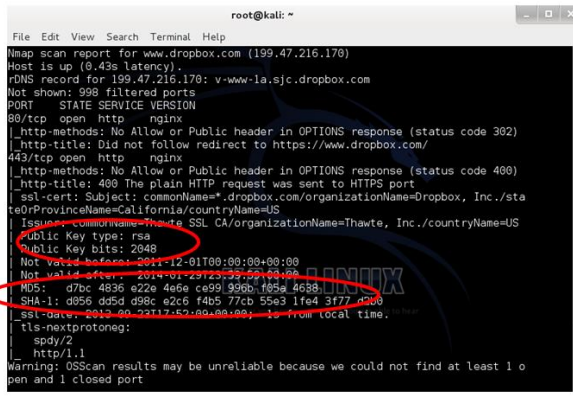

Figura 9 Uso de Herramienta WINHTTP

Método encontrado HTTP hacia HTTPS 2048 bits prácticamente invulnerables

12. Criptografía:

La combinación de la criptografía en el certificado digital nos da por lo tanto, que intentar romper un certificado RSA de 2048-bit SSL tomaría alrededor de 4,3 mil millones de veces más (usando el mismo proceso estándar de escritorio) que lo hace para una clave de 1024 bits. Se estima, por tanto, que el poder de computación de escritorio estándar tomaría 4294967296 x 1,5 millones de años para romper un certificado 2048-bit certificado SSL, o en otras palabras, tomaría un poco más de 6,4 cuatrillones de años.[6]

13. Conclusiones

1. Aunque el servicio *Dropbox* en nuestro estudio de seguridad haya arrojado datos satisfactorios los cuales nos podrían crear tranquilidad de usar este tipo de servicios hay que tener en cuenta que estamos arrendando un servicio en el caso de las cuentas con pago, pero en el caso de cuentas de acceso gratis la confidencialidad e integridad de nuestros datos están a cargo de la buena voluntad de terceras personas por lo que no podríamos exigir respuestas en el caso de pérdida, duplicación o uso de nuestros datos.

2. En el diseño seguro de almacenamiento en la Nube que posee Dropbox, debemos tener presente que esto implica, compartir los recursos almacenados, Para lo cual los administradores de la Nube han proporcionado un nivel satisfactorio de confidencialidad haciendo virtualmente imposible la captura de credenciales de autenticación con los ataques normalmente conocidos como hombre en el medio, ataques de fuerza bruta, ataques de explotación de confianza. Sin embargo un tema aparte es la Ingeniería social mediante la cual podríamos involuntariamente entregar nuestros datos de inicio de sesión.

15. Recomendaciones

1. El hecho de que nuestros datos abandonen su lugar de origen y viajen por redes desconocidas puede representar un riesgo en la privacidad de nuestros datos, de tal manera que se hace muy necesario el uso de la criptografía y jugará un papel protagónico en el uso de los servicios de la Nube por tal motivo de dan 3 recomendaciones para su uso en la Nube:

2. Protección de las conexiones entre los usuarios: El uso de Secure Sockets Layer (SSL) y Trasnport Layer Security (TLS) permiten que todos nuestros datos que viajen desde el servidor en la Nube hasta el usuario estén cifrados impidiendo el acceso a terceras personas incluso hasta cuando se utiliza una red WI-FI no segura

3. Protección de las conexiones entre los administradores del sistema y los servicios de la Nube: En este caso el uso Secure Shell (SSH) y Virtual Private Network (VPN) permitirá a los administradores del sistema o desarrolladores de las aplicaciones mantener un canal seguro de comunicación en la Nube

3. Protección de los datos utilizando Criptografía. Si utilizamos la Nube como un sistema de almacenamiento de datos es recomendable utilizar un nivel de cifrado adecuado para aquellos datos

sensibles que vayan hacer depositados en la Nube. [7]

16. Referencias

[1] Johnston Sam, File: Cloud_computing.svg, http:// www.wikipedia.org, fecha de consulta Julio 2013

[2] El Blog de Virtualizamos ,http://inbest.me/de-iaas-a-saas, fecha de consulta Julio 2013

[3] ENISA Agencia Europea de Seguridad de las Redes y de la Información, Beneficios, riesgos y recomendaciones para la seguridad de la información, 1st. Ed, 2009

[4] López Bravo Cristina, Departamento de Ingeniería Telemática, Universidad De Vigo, Seguridad en Internet , http://www-gris.det.uvigo.es/wiki/pub/Main/PaginaNST/seguridad-Clase1-NSTx.pdf

[5] LACNIC, el Registro de Direcciones de Internet Para América Latina y Caribe, Políticas de Administración de Recursos de Internet en el Área de Latinoamérica y el Caribe, http://lacnic.net/sp/politicas/2002-11-num_sis.html, fecha de consulta Noviembre 2013

[6] Engebretson Patrick, The Basics Hacking and Penetration Testing Ethical Hacking and Penetration Testing Made Easy, ELSEVIER 1st Ed 2011.

[7] Observatorio de la Seguridad de la Información de INTECO: Instituto Nacional de Tecnologías de la Comunicación, "Guía para empresas: seguridad y privacidad del cloud computing".