Trabajo Final Integrador

Titulo: INFORMATICA FORENSE Y SEGURIDAD EN LA NUBE

Autor: ING. RAUL OSCAR ROMERO

POSGRADO ESPECIALIZACIÓN EN INFORMÁTICA FORENSE

Facultad de ingeniería

Director:

ING. PABLO CROCI

01/09/2022

UNIVERSIDAD FASTA FACULTAD DE INGENIERÍA

Índice General

Índice de Ilustraciones

Resumen

En el presente trabajo final integrador se desarrollaron consideraciones sobre la nube privada Owncloud aplicando informática forense aplicado mediante la técnica de ingeniería inversa, para mitigar las brechas de seguridad.

Para la obtención de las consideraciones se utilizaron tres (3) escenarios: DFIR de la nube sin acceso físico, DFIR de la nube con acceso físico, Obtención de una imagen de la nube, en los cuales se utilizaron diferentes técnicas y herramientas para realizar las adquisiciones y/o información de memoria, logs, etc.

Los medios físicos utilizado son un servidor, un cliente y un teléfono celular. La topología de red adoptada fue Wi-Fi.

Se llevó a cabo mediante la realización de una estructura topológica emulando un ambiente real.

Se seleccionó para este trabajo, una situación empresa cliente (B2C).

Dado la experiencia y conocimiento de la existencia de vulnerabilidades, se optó por trabajar en el servidor y en el cliente con el Sistema Operativo Microsoft y el teléfono celular con Sistema Operativo Android.

Luego de visualizar los hallazgos en los escenarios antes mencionados se concluye que, la aplicación de estándares de seguridad, buenas prácticas resultaron ser efectivas y asertivas a la hora de mermar las brechas de seguridad.

Para evitar futuros ataques y/o brechas de seguridad, también es la concientización y capacitación para las organizaciones y/o usuarios que interactúen con los sistemas de la nube.

Palabras clave: estándares, informática forense, redes, seguridad de la información, vulnerabilidad, nube

Acrónimos

DFIR	**Digital Forensic Incident Response**
FBI	**Federal Bureau Investigation**
ISO	***International Organization for Standardization***
NIST	***National Institute of Standard and Technology***
ISO 27037	***International Standard Organization 27037***
ISO 27042	***International Standard Organization 27042***
TCP/IP	***Transport Control Protocol / Internet Protocol***
IAAS	***Infrastructure as a Service***
PAAS	***Platform as a Service***
SAAS	***Software as a Service***

Capítulo I – Introducción

1.1. Justificación del tema

Como se sabe, en la actualidad, la nube se está convirtiendo en un ambiente de trabajo común y cotidiano tanto para empresas como las organizaciones.

Por razones de costo, practicidad y accesibilidad las empresas están migrando información física a la nube.

Existen varios tipos de incidentes de seguridad en la nube y diferentes tipos de nube, como ser: pública, híbrida y privada.

El escenario planteado para este trabajo final es un escenario real y se toma como sistema operativo para análisis Microsoft Windows, debido a la experiencia y gran posibilidad de existencia de vulnerabilidades y/o hallazgos.

Para este trabajo se tomará un escenario real de nube privada, la que estará basada en la plataforma "Owncloud". La modalidad será el análisis de caso ex post.

1.2. Desafío o Problema

Actualmente las empresas u organizaciones se encuentran en constante crecimiento y eso conlleva a actualizarse con nuevas tecnologías. Una de estas es la "nube".

Si bien la nube no es una tecnología reciente, en Argentina, los usuarios están migrando hacia allí.

El objetivo de este trabajo será elaborar una serie de consideraciones para tener en cuenta para minimizar o mitigar las brechas de seguridad en la nube privada "Owncloud"[1] aplicando ingeniería inversa a partir del análisis forense de los escenarios posibles.

[1] OwnCloud es una aplicación de software libre del tipo Servicio de alojamiento de archivos, que permite el almacenamiento en línea y aplicaciones en línea.

La importancia de esto son las consecuencias que pueden causar pérdidas importantes tanto en la reputación como en lo económico.

1.3. Disparadores de la Investigación

La motivación para realizar este trabajo se origina en la gran cantidad de reportes de ciberataques, que ocurren en la actualidad en la nube de distinta índole.

Hace cinco años, muy pocas personas tenían archivos en la nube. Con el mundo cada vez más digital, esta tendencia está cambiando y ya hay muchos usuarios que almacenan sus datos allí. Lo hacen para registrar su trabajo y su información privada, así como sus recuerdos privados, como fotos. La nube se ha vuelto más importante para todos. Los ciberdelincuentes tienen sus ojos puestos en ella para obtener ganancias.

Los ciberdelincuentes saben lo importantes que son los servicios en la nube e intentarán apoderarse de ellos. Lo consiguen realizando ataques en la nube.

Los ataques a la nube están a la orden del día, y uno de los más recientes es el ransomware. En este tipo de ataques, los ciberdelincuentes cifran nuestros archivos y no podremos acceder a ellos. Si queremos recuperar estos datos, tendremos que pagar un rescate. Sin embargo, no es práctico hacer esto ya que no tiene garantía de que le darán el código para hacerlo.

Además, es posible que algunos archivos no se recuperen mientras se descifran; de lo contrario, sus archivos aún pueden estar infectados con virus, por lo que es posible que se le pida que pague otro rescate después. Los ataques en la nube pueden ser de varios otros tipos, como ataques DDoS, phishing y fuerza bruta, contra las credenciales, y también se pueden aprovechar las vulnerabilidades. (Lorenzo, 2021)

1.4. Propuesta

La propuesta es minimizar o mitigar las brechas de seguridad en la nube privada “Owncloud” aplicando informática forense mediante ingeniería inversa.

Como información adicional referido a la ingeniería inversa, se puede decir que, en casos de hacking ético, informática forense y ciberseguridad, trabajan o colaboran de manera conjunta, cuando se produce un incidente o un ataque de un hacker intruso.

1.5. Bases Teóricas

En este punto se verán las bases teóricas del presente trabajo de investigación, entre ellos, la historia y los conceptos de nube y sus tipos, la informática forense, sus herramientas y estándares.

Concepto de nube: El concepto básico de proporcionar recursos informáticos en una red global se remonta a la década de 1960. La idea de las "redes informáticas intergalácticas" fue introducida en la década de 1960 por JCR Licklider, cuya visión era ser universal.

El mundo se puede interconectar, el software y los datos se pueden acceder desde cualquier lugar. Otros expertos atribuyen el concepto científico de la computación en la nube a John McCarthy, quien propuso la idea de la computación como un servicio público, similar a las empresas de servicios que datan de la década de 1960.

Desde la década de 1960, la computación en la nube se ha desarrollado en varios ejes. Web 2.0 es el último desarrollo. Sin embargo, dado que Internet solo comenzó a proporcionar un ancho de banda significativo en la década de 1990, la computación en la nube ha sido un tipo de desarrollo tardío. Una de las primeras fases importantes de la computación en la nube fue la llegada de Salesforce.com en 1999, que fue pionera en el concepto de entregar aplicaciones comerciales a través de una página web simple. Esta empresa de servicios allanó el camino para que los profesionales y las empresas de software tradicionales publicaran sus aplicaciones en Internet.

El siguiente desarrollo fue Amazon Web Services en 2002, que ofrece una variedad de servicios basados en la nube que incluyen almacenamiento, computación e incluso inteligencia humana a través de Amazon Mechanical Turk. A finales de 2006, Amazon lanzó Elastic Compute Cloud (EC2) como un servicio comercial que permite a las pequeñas empresas y particulares alquilar ordenadores para ejecutar sus aplicaciones informáticas.

Otro hito importante ocurrió en 2009, cuando Google y otros comenzaron a ofrecer aplicaciones basadas en navegador. La contribución más significativa a la computación en la nube ha sido la aparición de las llamadas “aplicaciones asesinas” de gigantes tecnológicos como Microsoft y Google. A medida que estas empresas brindan sus servicios de manera segura y fácil a los consumidores, el efecto de “muerte” en sí mismo crea un mayor sentido de aceptación de los servicios en línea. Otro factor importante que ha permitido que la computación en la nube evolucione es la tecnología de virtualización, el crecimiento del ancho de banda de alta velocidad del espectro y los estándares globales de interoperabilidad de software. Con la difusión de la computación en la nube, su alcance se ha extendido más allá de unos pocos usuarios de Google Docs. Solo podemos comenzar a visualizar su alcance. Casi cualquier cosa se puede utilizar en la nube. (grandejosh, 2017)

En la ilustración 1 se visualiza la estructura de la nube. (Almudena Bernal Cremonesi, 2020)

Ilustración 1 - Estructura de la nube. (Almudena Bernal Cremonesi, 2020)

Nube: El termino computación en la nube se refiere a la computación basada en web. (Anonimo, 2020)

Es una herramienta informática que permite guardar archivos o datos en Internet. Este servicio es gestionado por un proveedor informático a través de las versiones comerciales gratuitas o de pago. La cantidad de almacenamiento online depende de lo que necesite el usuario en caso de pago, o si es gratuito a criterio del proveedor. En este caso, el proveedor del servicio, a través del sistema de almacenamiento, es el responsable de hacer una copia de seguridad de los archivos y asegurarse de que permanezcan en Internet. También son responsables de garantizar la disponibilidad si es necesario. Los usuarios pueden subir archivos a la nube desde dispositivos móviles y computadoras conectadas a Internet. (Fórmate.es, 2021)

En la ilustración 2 se visualiza otra forma de estructura de la nube. (Anonimo, 2020)

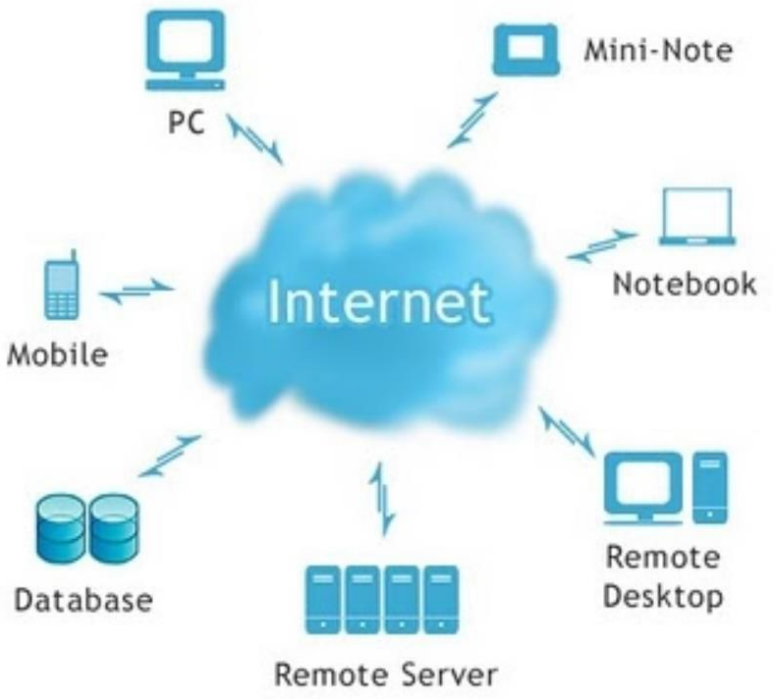

Ilustración 2 - Otra forma de Estructura de la nube. (Anonimo, 2020)

Tipos de nube: existe cuatro (4) tipos principales de nubes: (Anonimo, 2020)

- *Nubes personalizadas*: Estas son nubes creadas para satisfacer las necesidades de un sector específico, como salud o medios. Las nubes personalizadas pueden ser privadas o públicas.
- *Nubes públicas*: Las aplicaciones y los servicios basados en la nube que se ofrecen en una nube pública están a disposición de la población en general.
- *Nubes privadas*: Las aplicaciones y los servicios basados en la nube que se ofrecen en una nube privada están destinados a una organización o una entidad específica, como el gobierno.
- *Nubes hibridas*: Una nube híbrida consta de dos o más nubes (por ejemplo, una parte personalizada y otra parte pública); ambas partes son objetos separados, pero están conectadas mediante una única arquitectura.

En la ilustración 3 se visualizan los tipos de nube. (EGG, 2020)

Ilustración 3 - Tipos de nube. (Informatic, 2022)

Informática forense

Rodney McKemmish define informática forense como una técnica que utiliza un método para capturar, procesar e investigar información procedente de sistemas informáticos para que pueda ser utilizado en los tribunales. (McKemmish, 1999, p. 1)

En lo que respecta al FBI (de sus siglas en inglés, Federal Bureau of Investigation) (Standardization, n.d.), dicho organismo define a la informática forense como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados de manera electrónica y almacenados en medios informáticos. Se puede apreciar que ambas definiciones coinciden en algunos conceptos y que pueden complementarse. Uno de los objetivos principales del análisis forense es obtener evidencias que permitan llegar a conclusiones sin dar lugar a la duda.

Para finalizar, podemos decir que, la informática forense es la aplicación de técnicas científicas y analíticas especializadas en infraestructura tecnológica que permiten la identificación, preservación, análisis y presentación de datos que sean válidos dentro de procesos preventivos, legales o particulares.

Utilidad de la Informática Forense

La informática forense tiene muchos usos. Más aún, dado el aumento de las amenazas cibernéticas para las empresas y los usuarios debido al uso cada vez mayor de la tecnología que ahora está sucediendo en todos los niveles. Podemos destacar algunas instalaciones relacionadas: (EALDE, 2021)

- *Proporcionar evidencia durante los procedimientos legales*: en casos de manipulación del disco duro, robo de datos o ataque de malware, el análisis forense puede ser una evidencia vital en los procedimientos legales físicos.
- *Aportación de Evidencia en Negociación*: Podemos ver un ejemplo en el caso de la negociación colectiva, donde un trabajador puede demostrar que está haciendo su trabajo correctamente en base a los datos, y si se pueden extraer de su ordenador. También es posible lo contrario, y es el análisis forense el que determina que el empleado está incurriendo en conductas contrarias a su empresa.

- *Seguros de Internet*: Los seguros contra ataques informáticos son cada vez más populares. En este sentido, cuando se produce una brecha de seguridad, el profesional necesita reunir pruebas para ver si se debe aplicar el seguro. Es similar a lo que sucede en las evaluaciones de seguros de automóviles.

Herramientas forenses

Las herramientas forenses son las que nos permiten realizar los distintos tipos de análisis forenses.

Algunas de éstas son multiplataformas (se pueden ejecutar en cualquier tipo de Sistema Operativo), otras vienen incorporadas o embebidas en distribuciones Linux/Unix (LiveCD).

A continuación, se listan algunas herramientas forenses más relevantes y utilizadas por los peritos y/o analistas forenses:

- FTK Imager
- CAINE (COMPUTER AIDED INVESTIGATIVE ENVIRONMENT)
- TSUGURI
- DEFT LINUX y DEFT ZERO
- AUTOPSY DIGITAL FORENSICS
- MAGNET
- VOLATILITY
- WIRESHARK
- ENCASE
- RELATIVITY

A continuación, se visualizarán algunos logos o capturas de las herramientas de informática forense más relevantes:

En la ilustración 4 se visualiza el logo de la empresa EnCase Forensic (Champlain, 2013), en la ilustración 5 se visualiza una captura del software Autopsy Digital Forensics (Sacco, 2021),

Ilustración 4 - EnCase Forensics. (Champlain, 2013)

Ilustración 5 - Autopsy Digital Forensics. (Sacco, 2021)

En la ilustración 6 se visualiza captura del software Caine (Jimenez, GNU Linux, 2018),

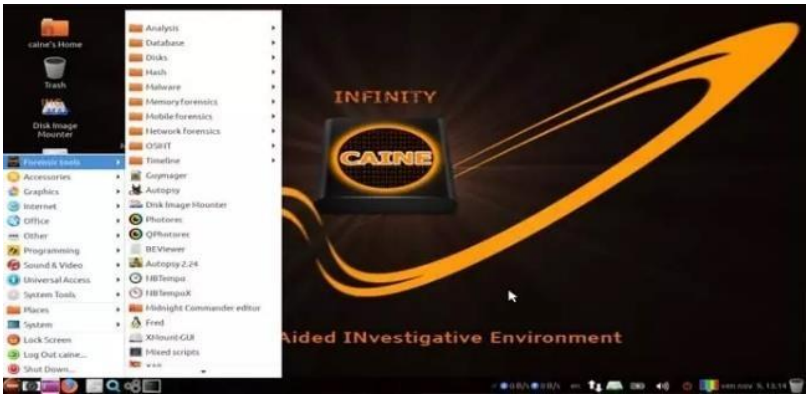

Ilustración 6 – CAINE (Jimenez, GNU Linux, 2018)

y en la ilustración 7 se visualiza el logo del software FTK Imager (Daza, 2021).

Ilustración 7 - FTK Imager

Tipos de análisis forenses

Existen varias modalidades para realizar un análisis forense informático, de los cuales se pueden mencionar algunos de ellos: (CPCI, 2019)

- *Análisis Forense de Equipos de Cómputo*: computadoras personales, notebooks, netbooks, memoria RAM.
- *Análisis Forense de Dispositivos Móviles*: teléfonos celulares, Smartphones, tablets.
- *Análisis Forense de Software*: software enlatado, software a medida, sistemas operativos.
- *Análisis Forense de Dispositivos Extraíbles*: disco rígido magnético, disco estado sólido, pendrive, memorias flash, medios ópticos (CD, DVD, Blue Ray, Mini-Disc), medios magnéticos (Tape BackUp).
- *Análisis Forense de Redes*: redes alámbricas e inalámbricas.

Estándares de Informática Forense

ISO / IEC 27037: 2012 – Recopilación de Evidencias Digitales

ISO / IEC 27037: 2012 estipula actividades específicas en el manejo de evidencia digital, que son la identificación, recolección, adquisición y preservación de evidencia digital potencial que puede ser de valor probatorio.

Orienta a las personas con respecto a situaciones comunes durante el proceso de manejo de evidencia digital y colabora con las organizaciones en los procedimientos disciplinarios y facilita el intercambio de potencial evidencia digital entre jurisdicciones.

También brinda orientación en Medios de almacenamiento digital utilizados en computadoras estándar como discos duros, disquetes, discos ópticos y magnetoópticos, dispositivos de datos con funciones similares como Teléfonos móviles, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria, Sistemas de navegación móvil (GPS), Cámaras digitales fijas y de video (incluyendo CCTV), Computadora estándar con conexiones de red, Redes basadas en TCP / IP y otros protocolos digitales, y Dispositivos con funciones similares a las anteriores. (27037:2012, 2012)

La norma ISO / IEC 27037: 2012 se basa en cuatro (4) principios, ellos son: (LÓPEZ RIVERA, 2012)

- *Aplicación de Métodos*: La evidencia digital debe recopilarse de la manera menos intrusiva posible, en un esfuerzo por preservar la autenticidad de la evidencia y, cuando sea posible, tener copias de seguridad.
- *Proceso Auditable*: Los procedimientos seguidos y los documentos producidos deben ser validados y verificados utilizando buenas prácticas profesionales. Se deben presentar evidencias y pruebas de lo realizado y sus resultados.
- *Proceso Reproducible*: Los métodos y procedimientos aplicados deben ser repetibles, verificables y defendibles con el nivel de conocimiento de quienes entienden el documento, quienes pueden confirmar y respaldar las acciones realizadas. Puede proteger el proceso.

- *Proceso Defendible*: Las herramientas utilizadas deben mencionarse y deben ser validadas y adaptadas en uso para los fines para los que se utilizan en el trabajo.

Para cada tipo de dispositivo, la norma divide el procedimiento o tramitación en tres procesos diferentes como modelo común para el manejo de la prueba: (LÓPEZ RIVERA, 2012)

- *La Identificación*: Este es el proceso de identificación de evidencia y consiste en localizar e identificar información potencial o evidencia en dos estados posibles, físico y lógico, dependiendo del estado de cada evidencia.
- *La Recolección y/o Adquisición*: Este proceso se define como la recopilación (confiscación y almacenamiento) de dispositivos y documentos que pueden contener pruebas que se están recopilando o la recopilación y copia de la información del dispositivo.
- *La Conservación/Preservación*: La prueba debe ser preservada para asegurar su utilidad, es decir, su autenticidad, para que luego pueda ser aceptada como prueba preliminar y completa, para que los procedimientos de este proceso sean claros. El propósito es preservar la cadena de custodia, integridad y autenticidad de la prueba.

ISO / IEC 27042: 2015 – Análisis e Interpretación de Evidencias Digitales

ISO / IEC 27042: 2015 proporciona orientación sobre el análisis e interpretación de la evidencia digital de una manera que aborda los problemas de continuidad, validez, reproducibilidad y repetibilidad. Encapsula las mejores prácticas para la selección, diseño e implementación de procesos analíticos y registra información suficiente para permitir que dichos procesos sean sometidos a un escrutinio independiente cuando sea necesario. Orienta acerca de los mecanismos adecuados para verificar en el equipo de investigación, el dominio y la competencia.

También proporciona un marco común, para los elementos analíticos e interpretativos del manejo de incidentes de seguridad de los sistemas de información, que se puede utilizar para ayudar a implementar métodos nuevos y brindar un estándar común y mínimo para la evidencia digital producida a partir de esas actividades. (27042:2015, 2015)

RFC 3227 – Directrices para la Recopilación de Evidencias y su Almacenamiento

En la solicitud de comentarios 3227 (de sus siglas en inglés RFC3227) propone que un "incidente de seguridad" como se define en RFC2828 “Internet Security Glossary” (Shirey, 2000) es un evento del sistema relevante para la seguridad en el que la política de seguridad del sistema se desobedece o se infringe de alguna otra manera. El propósito de este documento es proporcionar a los Administradores del sistema pautas sobre la recopilación y el archivo de evidencia relevante para dicho incidente de seguridad.

Si la recopilación de pruebas se realiza correctamente, es mucho más útil en aprehender al atacante, y tiene muchas más posibilidades de ser admisible en caso de enjuiciamiento. (Brezinski, 2002)

RFC 4810 – Requisitos del Servicio de Archivo a Largo Plazo

En la solicitud de comentarios 4810 (de sus siglas en inglés RFC4810) se propone que la durabilidad de los datos digitales se ve socavada por el progreso continuo y los cambios en varios frentes. La vida útil de los datos puede exceder la vida útil de los formatos y mecanismos utilizados para almacenar los datos. La vida útil de los datos firmados digitalmente puede exceder los períodos de validez de los certificados de clave pública utilizados para verificar las firmas o el período de análisis criptográfico de los algoritmos criptográficos utilizados para generar las firmas, es decir, el tiempo después del cual un algoritmo ya no proporciona las propiedades de seguridad previstas. Se requieren medios técnicos y operativos para mitigar estos problemas. Una solución debe abordar problemas como la vida útil de los medios de almacenamiento, la planificación ante desastres, los avances en criptoanálisis o las capacidades computacionales, los cambios en el software tecnología y asuntos legales. (C. Wallace, 2007)

Ingeniería inversa

La ingeniería inversa, en el ámbito de la informática forense, es un proceso que nos brinda la posibilidad de averiguar o identificar las causa raíz u origen de un incidente. En dicho proceso se solicitan copias de logs, adquisición de unidades de disco, dispositivos extraíbles, capturas de memoria ram, etc. (Garcia, 2019)

Este tipo de ingeniería, en la informática, se utiliza en la recuperación de datos buscando el origen de la perdida de la información.

La ingeniería inversa puede clasificarse en dos grupos:

- *Ingeniería Inversa de Software*: en este aspecto entran los productos diseñados para los sistemas operativos.
- *Ingeniería Inversa de Productos*: en este aspecto ingresan los productos físicos de dispositivos de ordenadores, tabletas, teléfonos inteligentes, incluyendo todos sus componentes electrónicos.

Tipos de ataques en la nube

Cada vez más usuarios utilizan el almacenamiento en la nube todos los días. La nube nos ofrece muchas posibilidades que se pueden aprovechar a diario. Los ejemplos más comunes son para: crear copias de seguridad, liberar espacio en otros dispositivos, hacer que los archivos estén disponibles en cualquier lugar. Ahora, todas estas cosas hacen que los piratas informáticos busquen aplicar sus ataques en los ejemplos antes mencionados.

Una de las formas principales de ataque de los ciber atacantes es el phishing, maniobra que utilizan para robar las credenciales de sus víctimas.

Con el tiempo el auge de los servicios en la nube, han aumentado los ataques y las técnicas más comunes, aplicadas por los ciber atacantes son: (Jimenez, Seguridad, 2020)

- Fuerza bruta
- Explotaciones de vulnerabilidades
- Servicios o tecnologías obsoletas.

1.6. Ventajas y Desventajas de la Nube

La utilización de la nube tiene sus ventajas y desventajas. A continuación, se mencionan algunas de ellas: (Anonimo, 2020) (Fórmate.es, 2021)

Ventajas:

- *Costos bajos en la infraestructura*: El uso del almacenamiento en la nube elimina la necesidad de sistemas potencialmente costosos. Además, esta herramienta le permite acceder a la memoria en gigabytes o terabytes de manera online, sin la necesidad de utilizar hardware a una tarifa mucho más económica a través de planes pagos o gratuitos.
- *Accesibilidad*: En cualquier lugar que se pueda lograr una conexión a Internet, podrá acceder a sus archivos sin ningún problema. Puede ser fácilmente productivo con este enfoque, que permite la portabilidad, que solo es posible en el entorno de red actual.
- *Recuperación de datos*: Si utilizamos un dispositivo normal para almacenar cualquier tipo de información y de repente deja de funcionar, existe la posibilidad de perderlo todo. Con el almacenamiento de datos en la nube, esto no tiene por qué suceder. La suplantación de disco físico de esta manera permite guardar archivos de forma segura, evitando problemas inesperados.
- *Privacidad y Seguridad*: los proveedores de almacenamiento en la nube de hoy en día están agregando capas de seguridad para protegerlos de personas que no deberían tener acceso a ellos. Por otro lado, pueden proteger archivos de desastres naturales, fallas del servidor o errores que los usuarios podrían tener que preservar.
- *Creación de nuevos modelos empresariales*: se puede acceder a las aplicaciones y recursos fácilmente, para que las empresas puedan reaccionar rápidamente a las necesidades de los clientes.

Desventajas:

- *Conexión a Internet*: Para un sistema basado en la nube, es indispensable contar con acceso a internet para poder acceder a los archivos. De todos modos, si la velocidad de internet que se está utilizando es lenta, probablemente surjan inconvenientes a la hora de querer ver o descargar los archivos almacenados. Y sencillamente, sino tener acceso a internet, no es posible acceder a ellos de ninguna manera.
- *Costos adicionales*: Al ser un sistema que necesita mucho mantenimiento, los proveedores de estos servicios pueden agregar costos adicionales según el volumen de subidas o descargas de archivos a la nube. Esto sucede en algunas plataformas en las que los usuarios acceden con mucha frecuencia a ciertos archivos.
- *Hardware*: Aunque pensamos que con esto estamos eliminando por completo la dependencia de dispositivos físicos, la realidad es que no es así. Aunque puedas acceder a ellos a través de una conexión en red, muchos proveedores utilizan discos duros para poder prestar el servicio de guardado de datos en la nube.
- *Vulnerabilidad a ciberataques*: Según la arquitectura de seguridad del proveedor de la nube, uno de los beneficios más importantes es que estos archivos pueden no estar completamente seguros si se exponen. Esto afecta especialmente a las grandes empresas que almacenan grandes cantidades de datos en la nube y puede provocar problemas de pérdida de información e incluso pérdidas económicas.
- *Privacidad o Confidencialidad*: Cuando se cargan archivos en alguna plataforma de almacenamiento de archivos, automáticamente pasan a ser responsabilidad de las terceras partes. Las empresas de alojamiento están trabajando actualmente para proporcionar a los usuarios las soluciones de privacidad. Últimamente, sin duda alguna, los servicios en la nube se han convertido en una opción muy popular en la era digital. Las grandes

empresas hoy en día también utilizan este tipo de herramientas, al igual que los usuarios, ya sea a través de proveedores de servicio tales como, Google Drive, Office 365, Dropbox y cualquier otra plataforma popular en el mundo. El almacenamiento online proporciona copias de seguridad, lo cual es muy útil para cualquier usuario y/o empresa. No se necesita monitorear o administrar constantemente sus archivos, el proveedor de servicios se encarga de su mantenimiento y considerará los riesgos, pero no hay que olvidar encontrar uno que sea seguro y que pueda satisfacer sus necesidades.

1.7. Arquitectura de la nube

La arquitectura de la nube es cómo se combinan los componentes tecnológicos para crear una nube, en la que los recursos se agrupan mediante tecnología de virtualización y se comparten en una red. Los componentes de la arquitectura de la nube incluyen: (VMware, 2022)

- Plataforma front-end (el cliente o dispositivo utilizado para acceder a la nube)
- Plataforma back-end (servidores y almacenamiento)
- Modelo de entrega basado en la nube
- La red

1.8. Ventajas de la arquitectura de la nube

La arquitectura de computación en la nube permite a las organizaciones reducir o eliminar su dependencia de las redes de área local, la infraestructura de almacenamiento, servidores y terciarización de los servidores.

Las organizaciones que adoptan una arquitectura de nube a menudo migran sus recursos informáticos a la nube pública. Esto elimina la necesidad de servidores y almacenamiento local, y reduce la necesidad de espacio físico, enfriamiento del centro de datos y energía, que reemplaza con los costos mensuales de TI.

El cambio de un modelo de inversión a un modelo operativo es una de las principales razones por las que la computación en la nube es tan popular hoy en día. (VMware, 2022)

1.9. Tipos de arquitectura de nube

Existen tres estilos principales de arquitectura en la nube que facilitan a las organizaciones la migración a la nube. Cada uno de ellos ofrece ciertas ventajas y características clave: (VMware, 2022)

- *Software como servicio (SaaS)*: los proveedores de arquitectura SaaS administran la entrega y el mantenimiento de aplicaciones y software para organizaciones a través de Internet. Esto elimina la necesidad de que el usuario final implemente el software localmente. Por lo general, se accede a las aplicaciones SaaS a través de una interfaz web que está disponible desde una variedad de dispositivos y sistemas operativos.
- *Plataforma como servicio (PaaS)*: con este modelo de nube, el proveedor de servicios proporciona una plataforma informática y una pila de soluciones, que a menudo incluye middleware. Las organizaciones pueden aprovechar esta plataforma para crear aplicaciones o servicios. El proveedor de servicios en la nube proporciona la red, los servidores y el almacenamiento necesarios para alojar una aplicación, mientras que el usuario final supervisa la implementación y la configuración del software.
- *Infraestructura como servicio (IaaS)*: en este modelo de nube en su forma más simple, un proveedor externo proporciona la infraestructura necesaria, eliminando la necesidad de que la organización compre servidores, redes o dispositivos de almacenamiento. Por otro lado, las organizaciones gestionan su software y aplicaciones, y solo pagan por la capacidad que necesitan en cada momento.

En la ilustración 8 se visualizan los tipos de modelos de servicio en la nube. (Stackscale, 2020)

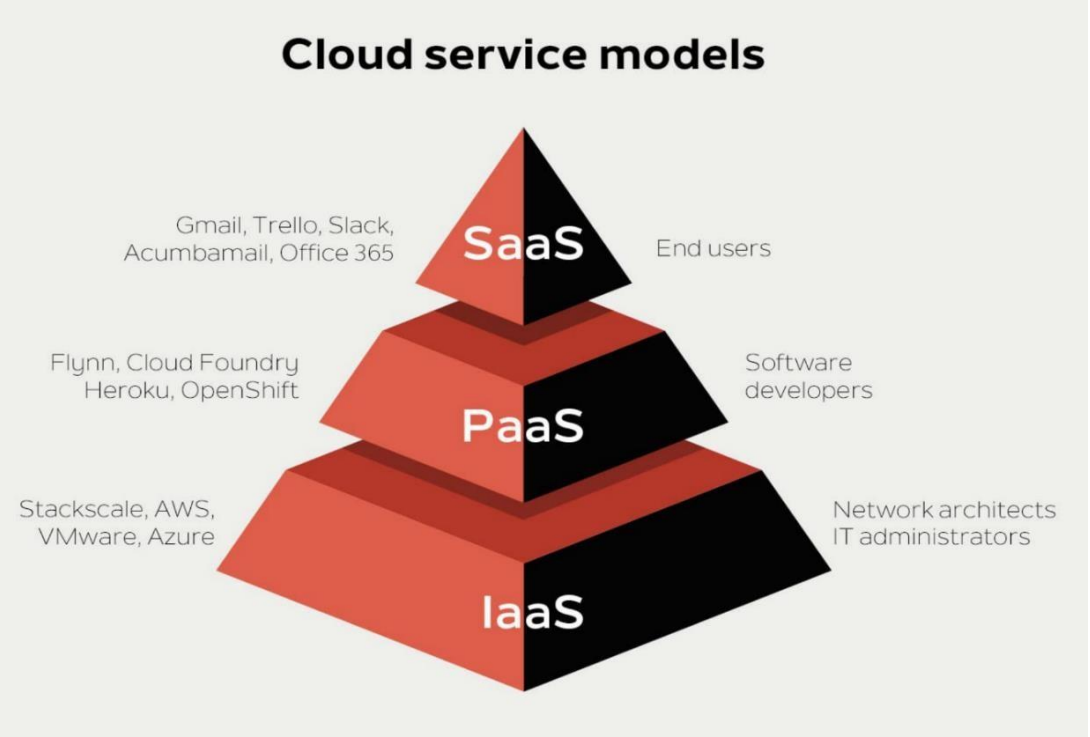

Ilustración 8 - Cloud Service Models (Stackscale, 2020)

Capítulo II – Objetivos del Trabajo

Se plantean los objetivos generales y específicos del análisis forense de la nube privada Owncloud.

2.1. Objetivos Generales

El objetivo general de la presente investigación es obtener consideraciones del análisis forense de la nube privada Owncloud.

2.2. Objetivos Específicos

Los objetivos específicos de la presente investigación son:

- Proponer alguna metodología de trabajo de mitigación de brechas en seguridad.
- Proponer tanto a las empresas como a las organizaciones mantener y actualizar normas y estándares relacionados con la seguridad de la información en la nube.

Capítulo III – Desarrollo

3.1. Ambiente de trabajo o Laboratorio

Para la realización de la presente investigación se creó un ambiente de laboratorio. Para ello se utilizaron dos (2) equipos de cómputo de distintas características técnicas, un teléfono celular para la creación de la nube privada y el otro equipo para realizar el análisis forense de los logs de actividades y otras muestras obtenidas de las ejecuciones de las herramientas forenses.

Luego con los equipos de cómputo, se realizó una conexión de red Cliente-Servidor. Uno de los equipos de cómputo cumplió con la función de Servidor, el otro equipo de cómputo y el teléfono celular cumplieron la función de Clientes.

3.2. Especificaciones técnicas de los equipos

Las características técnicas de los equipos son:

Servidor

Especificaciones del dispositivo

- Procesador: Intel ® Celeron ® CPU N3060 @ 1.60GHz
- RAM instalada: 4.00 GB
- Id. del dispositivo: 4DD207f3-8F3A-4CE7-B829-CD3153DAA878
- Id. del producto: 00380-00000-00001-AA671
- Tipo de sistema: Sistema Operativo de 64 bits, procesador x64
- Lápiz y entrada táctil: la entrada táctil no está disponible para esta pantalla.

Especificaciones del Sistema Operativo

- Edición: Windows 10 Pro Education
- Versión: 21H1
- Se instaló: 9/6/2022

- Compilación del SO: 19043.1776
- Experiencia: Windows Feature Experience Pack 120.2212.4170.0

Cliente

Especificaciones del dispositivo

- Procesador: Intel(R) Core(TM) i7-4720HQ CPU @ 2.60GHz 2.59 GHz
- RAM instalada: 16.0 GB (15.9 GB usable)
- Id. del dispositivo: 687CAAD2-5AFB-4EB3-9312-AE64AC29C797
- Id. del producto: 00325-95835-29402-AAOEM
- Tipo de sistema: 64-bit operating system, x64-based processor
- Lápiz y entrada táctil: Touch support with 10 touch points.

Especificaciones del Sistema Operativo

- Edición: Windows 10 Home
- Versión: 21H2
- Se instaló: 11/3/2020
- Compilación del SO: 19044.1776
- Experiencia: Windows Feature Experience Pack 120.2212.4180.0

Teléfono Celular

Especificaciones del dispositivo

- Modelo Nombre: Galaxy S22 Ultra
- Modelo Numero: SM-S908E
- Fabricante: Samsung
- Memoria RAM: 12 GB
- Memoria Interna: 256 GB
- Velocidad CPU: 2.8 GHz
- Tipo CPU: Octa-Core

Especificaciones del Sistema Operativo

- One UI Version: 4.1

- Android Version: 12
- Kernel Version: 5.10.43-android12-9-24096951-abS908EXXS2AVDD#1
- SE for Android Status: Enforcing, SEPF_SM-S908E_12_0001
- Service Provider Software Version: SAOMC_SM-S908E_OWO_ARO_12_0016

Conectividad

- Interfaz USB: USB Tipo C
- Versión USB: USB 3.2 Gen 1
- Localización: GPS, Glonass, Beidou, Galileo, QZSS
- Auriculares: USB Type-C
- MHL: No
- Wi-Fi: 802.11 a/b/g/n/ac/ax 2.4G+5GHz+6GHz, HE160, MIMO, 1024-QAM
- Wi-Fi Direct: Sí
- Versión Bluetooth: Bluetooth v5.2
- NFC: Sí
- UWB (Ultra Wideband): Sí
- PC Sync.: Smart Switch (PC version)

3.3. Herramientas forenses

Para este trabajo se utilizó la herramienta de código abierto llamada “Bento” en su versión portable.

De la suite “Bento” se utilizaron las siguientes aplicaciones:

- RamCapture x64
- HashMyFiles x64
- WinAudit
- ServiWin x64

- Binalyze ACQUIRE
- Windows Live Response Collection
- CurrPorts x64
- LiveTcpUdpWatch x64
- ChromePass

Otra herramienta forense utilizada:

- Wireshark

3.4. Aplicaciones

Las aplicaciones que se utilizaron para este trabajo fueron:

- Owncloud
- WampServer
- Autopsy Digital Forensic
- FTK Imager
- Wireshark

3.5. Escenarios

Para este trabajo de investigación se plantearon los siguientes escenarios:

- *Escenario 1 – DFIR de la nube sin acceso físico*: para este escenario se solicitaron logs de actividades y capturas de información desde las herramientas forenses, dicha información surge del servidor. Se pide la información de esta manera ya que no se cuentan con las credenciales de ingreso al servidor. Se indica al administrador del servidor ejecutar las herramientas forenses antes mencionadas desde la SUITE BENTO en su versión portable.

- *Escenario 2 – DFIR de la nube con acceso físico*: para este escenario se tomó el tráfico de red desde el cliente.
- *Escenario 3 – Obtención de imagen de la nube*: para este escenario, se solicitó la adquisición del dispositivo de almacenamiento del servidor. La misma se realizó con la herramienta forense FTK Imager.

Capítulo IV – Análisis de Escenarios

En este capítulo, se tratan la obtención de información de los escenarios y el análisis correspondiente de cada escenario.

4.1. Obtención de la información

Escenario 1 – DFIR de la nube sin acceso físico

En este escenario se solicitó ejecutar las siguientes herramientas forenses:

- RamCapture x64: obteniendo el archivo 20220621.mem
- HashMyFiles x64: obteniendo el archivo Hash List.html
- WinAudit: obteniendo el archivo DESKTOP-9OMVE0T_WinAudit.html
- ServiWin x64: obteniendo el archivo ServWin64.txt
- Binalyze ACQUIRE: obteniendo el archivo ACQUIRE.Report.2022-06-21.pdf
- CurrPorts x64: obteniendo el archivo TCP_UDP Ports List.html
- LiveTcpUdpWatch x64: obteniendo el archivo LiveTcpUdpWatch.txt
- ChromePass: obteniendo el archivo ChromePass_DATA.txt

Escenario 2 – DFIR de la nube con acceso físico.

En este escenario en el equipo de cómputo cliente se ejecutó la herramienta forense wireshark realizando una captura de tráfico contra el servidor obteniendo el archivo Captura_Trafico_Cli_Ser_Sync.pcapng

Escenario 3 – obtención de imagen de la nube.

En este escenario se solicitó al administrador del servidor ejecutar desde un dispositivo USB el archivo AccessData FTK Imager.exe de la herramienta forense FTK Imager.

Se han obtenido archivos Owncloud.E01 hasta el archivo Owncloud.E17. Dicha adquisición se analizará con la herramienta Autopsy Digital Forensic.

4.2. Análisis de la información obtenida

4.2.1. Escenario 1 – DFIR de la nube sin acceso físico

En este escenario, se solicitó al administrador del servidor ejecución de las herramientas forenses, ya que como usuario normal no es posible acceder al servidor.

Se realizo un DFIR de la nube sin acceso físico, para ello se ejecutó la herramienta RamCapture x64 con ella se obtiene el archivo 20220621.mem, para investigar su contenido se utiliza el módulo "imageinfo" de la aplicación "volatility". La ejecución de dicho comando no arroja información relevante.

Luego se verificó la integridad de los archivos obtenidos mediante el hash de los archivos, para ello se ejecutó la aplicación HashMyFiles x64 y para verificar que los hashes son los correctos se realizó la verificación con la aplicación MD5 & SHA Checksum Utility 2.1[2].

Paso siguiente se ejecutó la aplicación "WinAudit", con ella se obtuvo información detallada de la configuración de: software instalado, seguridad, accesos de usuarios y grupos, adaptadores de red, puertos.

Para entendimiento del tipo de servidor se ejecutó la aplicación "Binalyce Acquire", que brindo información tales como: sistema operativo, memoria ram, log de actividades, información del registro del sistema operativo, aplicaciones instaladas, navegadores, cace, información de configuración de redes y adaptadores de red.

Para obtener información más especifica de la información de redes se ejecutó la aplicación "CurrPorts x64" obteniéndose información relevante de puertos, PID de aplicaciones, direcciones IP, etc.

Y como complemento para la información de redes se ejecutó la aplicación "LiveTcpUdpWatch x64" que nos brindó detalles de los PID de las aplicaciones relevantes, tales como: Apache, MySql y Owncloud.

Para visualizar información más detallada del "Escenario 1", ver Anexo I - Escenario 1 – DFIR de la nube sin acceso físico.

[2] https://md5-sha-checksum-utility.apponic.com/download/

4.2.2. Escenario 2 – DFIR de la nube con acceso físico.

En este escenario, se solicitó al usuario la ejecución de las herramientas forenses en el equipo cliente.

Se realizó un DFIR de la nube con acceso físico en el equipo de cómputo cliente, en el que se ejecutó la herramienta forense wireshark realizando una captura de tráfico de red contra el servidor obteniendo el archivo “Captura_Trafico_Cli_Ser_Sync.pcapng”.

La captura de trafico de red se realizó al momento de la sincronización con el equipo de cómputo cliente.

De la captura de tráfico obtenida, se visualiza comunicación principal entre la dirección IP 192.168.100.24 que corresponde al servidor y la dirección IP 192.168.100.6 que corresponde al cliente.

Se instalo la aplicación cliente de Owncloud, en la cual se pudo verificar el proceso de sincronización de la información entre el cliente y el servidor, la cual dio resultado satisfactorio.

Para el caso del dispositivo mobile, se procedió a instalar el software cliente correspondiente para el teléfono celular, obtenida del Play Store de Android, luego se realizó la sincronización correspondiente de manera satisfactoria.

Para visualizar información más detallada del “Escenario 2”, ver Anexo I - Escenario 2 – DFIR de la nube con acceso físico.

4.2.3. Escenario 3 – Obtención de imagen de la nube.

En este escenario, se solicitó al administrador del servidor ejecución de las herramientas forenses, ya que como usuario normal no es posible acceder al servidor.

Se realizo un DFIR de obtención de imagen de la nube, para ello se ejecutó la herramienta “FTK Imager”, con ello se realizó la adquisición forense del servidor.

El análisis de la adquisición se realizó con la aplicación “Autopsy Digital Forensics”. La información obtenida fue la siguiente: evidencia física del disco rígido, datos de inicio y fin de la adquisición, cantidad de volúmenes de la adquisición, software instalado,

documentos recientes, cuentas de usuario del sistema operativo, cuentas tipo web, cuentas web, historial web.

Para visualizar información más detallada del “Escenario 3”, ver Anexo I - Escenario 3 - Obtención de imagen de la nube.

Capítulo V – Hallazgos

Para concluir el presente trabajo final integrador a continuación las estimaciones o conclusiones de los escenarios.

5.1. Escenario 1 – DFIR de la nube sin acceso físico

En este escenario se identificó actividades de conectividad en la cual se visualiza una dirección IP (192.168.100.17) correspondiente a un dispositivo.

Se verifica presencia de los servicios de Apache, MySql que trabajan con la aplicación Owncloud (también se verifica la aplicación instalada).

A nivel sistema operativo del servidor la cuenta Administrador se encuentra deshabilitada pero no está renombrada.

El usuario administrador y el usuario local no tienen configurada una contraseña ni bloqueo del equipo con el protector de pantalla.

Se verifica que los puertos 80 y 443 están abiertos.

5.2. Escenario 2 – DFIR de la nube con acceso físico.

En este escenario se detecta tráfico entre el cliente y el servidor y también una salida a internet de procedencia desconocida.

Se verifica que cualquier tipo de dispositivo puede conectarse al servidor con la URL del localhost que se comparte desde el servidor.

Dicha URL utiliza el puerto 80 ya que la URL comienza con http://, no utiliza SSL.

Se detectó un proceso denominado “UNKNOWN” que tiene comunicación con una dirección IP desconocida.

5.3. Escenario 3 – obtención de imagen de la nube.

En este escenario se detectó información nueva y otras coincidente con el escenario 1. La información detectada relevante es:

- Los usuarios y tipos de usuarios
- Software instalado (para la nube privada)
- Navegadores utilizados

Parte de la información nueva hace referencia a los documentos recientes, ello se aprecia en el punto 4.2.3, Tabla 13 en la cual se visualiza la ejecución de la herramienta forense FTK Imager, utilizada para la adquisición in live del servidor. También se puede visualizar acceso al archivo de configuración de la aplicación Apache.

Otra parte de la información nueva hace referencia al historial web, ello se aprecia en el punto 4.2.3, Tabla 17 en la cual se visualiza navegación en a distintas URLs que hacen referencia a las carpetas de almacenamiento de la nube privada Owncloud. Algunas de las URLs de referencia son:

- http://localhost/owncloud/
- http://localhost/owncloud/index.php
- http://localhost/owncloud/index.php/apps/files/
- http://localhost/owncloud/index.php/apps/files/?dir=%2Fmusic
- http://localhost/owncloud/index.php/apps/files/?dir=%2Fdocuments

Para verificar que dichas URLs pertenecen a las carpetas de almacenamiento de la nube privada Owncloud, se compararon las URLs con la ilustración 22 en el punto 4.2.2 en la cual se visualiza la sincronización del teléfono celular con el servidor de Owncloud.

Para más información ver Anexo I – Autopsy Export.rar.

Conclusión

Para concluir con el presente trabajo de final, al haber trabajado en una red Wi-Fi y en base a los hallazgos se recomienda segmentar una red para mayor seguridad de la nube privada.

En dicha recomendación se tendrá más control del tráfico entrante y saliente del servidor al momento de la sincronización de los clientes, ya sea con un equipo de cómputo o un teléfono celular.

Como se pudo verificar, en el Sistema Operativo Microsoft, existen vulnerabilidades que lo dejan muy expuesto, por lo que, en parametrización y seguridad en el servidor se recomienda utilizar un sistema operativo de distribución GNU/Linux (Debian, Ubuntu, Mint, etc.) en ella poder montar los servicios de mysql y apache, los cuales son nativos para la distribución antes mencionada. Se recomienda también realizar la instalación de la nube privada bajo la convención de línea de comando por consola, como alternativa por falta de conocimiento es válido también una distribución con entorno gráfico.

Cabe destacar también que la aplicación Owncloud tiene sus últimas versiones disponibles compatibles para distribuciones Linux o Debian.

Para el caso de no aceptar trabajar con la distribución antes recomendada, es válido también poder trabajar con un sistema operativo Windows.

En lo que a instalación de los servicios respecta, queda en claro que para el entorno Windows, la aplicación Owncloud no es recomendable, ya que no se encuentra actualizada lo cual genera riegos de vulnerabilidades y posibles ataques cibernéticos, pudiendo producir daños reputacionales y económicos, tanto a la organización como a los clientes.

Al no estar actualizada la versión de Owncloud para el sistema operativo Windows, también implica trabajar con versión no actualizada u obsoleta de las aplicaciones php, mysql y apache, siempre que se aplique al servidor.

Para el caso de seguir optando por usar servidores con sistema operativo Windows se recomienda adoptar las medidas de seguridad basadas en estándares y buenas prácticas.

Para más información ver Anexo II – CIS Control v8.

Anexo

1. Escenario I

Escenario 1 – DFIR de la nube sin acceso

2. Escenario II

Escenario 2 – DFIR de la nube con acces

3. Escenario III

Escenario 3 - Obtención de image

Anexo

1. Hash List

Hash List.html

2. Acquire Report

ACQUIRE.Report.2022-06-21.pdf

3. LiveTcpUdpWatch

LiveTcpUdpWatch.txt

4. TCP_UDP Ports List

TCP_UDP Ports List.html

5. CIS Control v8

CIS_Controls_v8_Online.22.02.pdf

CIS_Controls_Version_8.xlsx

6. Análisis Autopsy

Autopsy Export.rar

Bibliografía

27037:2012, I. (October de 2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. Obtenido de Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence: https://www.iso.org/standard/44381.html - Reviewed 2018 - https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

27042:2015, I. (Jun de 2015). *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*. Obtenido de Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence: https://www.iso.org/standard/44406.html - https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en

Almudena Bernal Cremonesi, A. S. (Marzo de 2020). *Grupo 9 de Tecnología*. Obtenido de CLOUD COMPUTING: https://gr9iacav.wordpress.com/nuestro-trabajo/

Anonimo. (1 de Octubre de 2020). *Internet en la vida cotidiana*. Obtenido de La Nube: https://sites.google.com/site/conceptodeinternetcdb/la-nube

Brezinski, D. &. (February de 2002). *RFC3227: Guidelines for Evidence Collection and Archiving.* Obtenido de RFC3227: Guidelines for Evidence Collection and Archiving.: https://dl.acm.org/doi/pdf/10.17487/RFC3227

C. Wallace, U. P. (March de 2007). *RFC4810: Long-Term Archive Service Requirements.* Obtenido de RFC4810: Long-Term Archive Service Requirements: https://www.hjp.at/doc/rfc/rfc4810.html

Champlain. (5 de Julio de 2013). *THE LEAHY CENTER FOR DIGITAL FORENSICS & CYBERSECURITY*. Obtenido de Painting a Timeline with EnCase: https://leahycenterblog.champlain.edu/2013/07/05/painting-timeline-encase/

CPCI. (23 de 08 de 2019). Perito Informático Forense. *ADQUISICIONES FORENSES Y EXTRACCIONES DE DATOS*. Buenos Aires, Buenos Aires, Argentina: CPCI .

Daza, S. (16 de Octubre de 2021). *https://behacker.pro/*. Obtenido de ¿Cómo crear una Imagen Forense de una MicroSD con FTK Imager?: https://behacker.pro/como-crear-una-imagen-forense-de-una-microsd-con-ftk-imager/

EALDE. (25 de Junio de 2021). *CIBERSEGURIDAD Y RIESGOS DIGITALES*. Obtenido de Qué es la informática forense y qué utilidad tiene en gestión de riesgos: https://www.ealde.es/informatica-forense/

EGG, P. (13 de Mayo de 2020). *Administración de dispositivos móviles de la elasticidad de los servicios web de la computación en la nube, datos grandes de computación en la nube, azul, Red de computadoras png*. Obtenido de Administración de dispositivos móviles de la elasticidad de los servicios web de la computación en la nube, datos grandes de computación en la nube, azul, Red de computadoras png: https://www.pngegg.com/es/png-ctsnq

Fórmate.es. (27 de Junio de 2021). *formate*. Obtenido de Almacenamiento en la nube: Ventajas y Desventajas: https://www.formate.es/blog/consejos/almacenamiento-en-la-nube/

Garcia, L. (26 de Septiembre de 2019). *OnRetrieval*. Obtenido de Ingeniería Inversa en Recuperación de Datos: https://onretrieval.com/ingenieria-inversa-en-la-recuperacion-de-datos/

grandejosh. (16 de Junio de 2017). *Cloud Computing*. Obtenido de Computación en la Nube: https://nubecomputingblog.wordpress.com/historia-del-cloud-computing/

Informatic, T. (16 de Marzo de 2022). *Características de la nube privada ¡Otro tipo de nube!* Obtenido de Características de la nube privada ¡Otro tipo de nube!: https://vidabytes.com/caracteristicas-de-la-nube-privada/

Jimenez, J. (12 de Noviembre de 2018). *GNU Linux*. Obtenido de CAINE 10; conoce todas las novedades de esta distro para análisis forense: https://www.redeszone.net/2018/11/12/caine-10-novedades-distro-analisis-forense/

Jimenez, J. (9 de Marzo de 2020). *Seguridad*. Obtenido de Técnicas de ataques a la nube que debes conocer: https://www.redeszone.net/tutoriales/seguridad/tecnicas-atacar-servicios-nube/

LÓPEZ RIVERA, R. (23 de Octubre de 2012). *Perito Informático y Tecnológico – PeritoIT*. Obtenido de ISO/IEC 27037:2012 Nueva norma para la Recopilación de Evidencias.: https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/

Lorenzo, J. A. (15 de Diciembre de 2021). *RZ Redes Zone*. Obtenido de Seguridad: https://www.redeszone.net/noticias/seguridad/cuales-principales-ataques-nube/

McKemmish, R. (June de 1999). *AUSTRALIAN INSTITUTE OF CRIMINOLOGY TREND & ISSUES IN CRIME AND CRIMINAL JUSTICE N 118.* Obtenido de What is Forensic Computing: https://aic.gov.au/publications/tandi/tandi118

Ranchal, J. (17 de Mayo de 2022). *https://www.muycomputer.com/*. Obtenido de Kali Linux 2022.2, nueva versión de la distro especializada en seguridad informática: https://www.muycomputer.com/2022/05/17/kali-linux-2022-2/

Romero, R. O. (8 de Agosto de 2021). Informática Forense, Seguridad y Estándares en Sistemas Industriales e Infraestructuras Críticas. *Informática Forense, Seguridad y Estándares en Sistemas Industriales e Infraestructuras Críticas*. Ciudad Autonoma de Buenos Aires, Buenos Aires, Argentina.

Sacco, L. (27 de Diciembre de 2021). *tus clases* . Obtenido de Autopsy, una herramienta de análisis digital forense: https://www.tusclases.com.ar/blog/autopsy-herramienta-analisis-digital-forense

Shirey, R. (May de 2000). *RFC2828: Internet security glossary.* Obtenido de RFC2828: Internet security glossary.: https://dl.acm.org/doi/pdf/10.17487/RFC2828

Stackscale. (14 de Abril de 2020). *Main cloud service models: IaaS, PaaS and SaaS*. Obtenido de Cloud Service Models: https://www.stackscale.com/blog/cloud-service-models/

Standardization, I. -I. (s.f.). *ISO - International Organization for Standardization*. Obtenido de STANDARDS: https://www.iso.org/standards.html

VMware. (7 de Junio de 2022). *Topics*. Obtenido de La arquitectura de nube en una red: https://www.vmware.com/es/topics/glossary/content/cloud-architecture.html#:~:text=La%20arquitectura%20de%20nube%20es,se%20comparten%20en%20una%20red