ANALISIS FORENSE A PAQUETES DE DATOS EN LA RED LAN DE LA UNIVERSIDAD TECNOLOGIA EQUINOCCIAL COMO APORTE AL CUMPLIMIENTO DE LAS NORMAS PCI-DSS

Ing. Mario Ron, Ing. William Chumi, Ing. Daniel Flores

Universidad de las Fuerzas Armadas ESPE, Quito – Ecuador, mbron@espe.edu.ec

Universidad de las Fuerzas Armadas ESPE, Quito – Ecuador, guillermokike@hotmail.com

Universidad de las Fuerzas Armadas ESPE, Quito – Ecuador, jdflores248@hotmail.com

RESUMEN

Este trabajo no solo representa un análisis forense al interior de la Universidad Tecnológica Equinoccial, sino también una idea aproximada del estado actual en el que se encuentra la institución educativa como institución participante en el procesamiento, transmisión o almacenamiento de información de tarjetas de crédito en la aplicación del estándar Payment Card Industry – Data Security Standard (PCI - DSS), la cual tiene como finalidad la reducción del fraude relacionado con las tarjetas de crédito e incrementar la seguridad de estos datos. Previamente se realizó una evaluación en base a los requisitos que expone la norma para determinar el nivel de cumplimiento de la institución a nivel general de todos los controles de la norma PCI – DSS, teniendo en cuenta que el estándar se compone de controles físicos, lógicos y documentales. Luego del cual se realizó una búsqueda potencial de datos de tarjetas de crédito siendo esta la labor más importante ya que el núcleo del estándar es la protección de datos de tarjetas de crédito procesados, almacenados o transmitidos a través de la red, para lo cual se utilizó herramientas OpenSource para la identificación de datos de tarjeta de crédito en tráfico a través de la red LAN no cifrados ni encriptados con lo cual se determinó que la institución no cumple diferentes requisitos de la norma. Finalmente se generó un plan de acción basados en la norma para la ejecución dentro de la Universidad y gestionar los riesgos identificados.

Palabras Claves: Análisis Forense, Payment Card Industry – Data Security Standard (PCI - DSS), OpenSource, Red LAN.

ABSTRACT

This work represents not only a forensic analysis into the Universidad Tecnológica Equinoccial but also a rough idea of the current state of the educative institution, as a participant institution in the processing, transmission, or storage of information related

to credit cards, in the application of the standard Payment Card Industry – Data Security Standard (PCI-DSS), which has the purpose of reducing credit card fraud and increasing data security. An evaluation based on the requisites set by the standard was previously done to determine the level of attainment of the institution on a general level to all the controls of the norm PCI – DSS, taking in consideration that this standard consists of physical, logical, and documental controls. A potential research of credit card data was then done as this was the most important task since the main focus of the standard is the protection of credit card data that has been processed, stored, or transmitted through the internet. OpenSource tools were used to identify non-encoded and unencrypted credit card data that was trafficking through the LAN; it was then determined that the Institution does not comply with several requisites of the norm. Finally, a plan of action based on the standards was made to be executed within the University and to manage the identified risks.

Key Words: Forensic Analysis, Payment Card Industry – Data Security Standard (PCI-DSS), LAN network.

1. INTRODUCCIÓN

El presente trabajo tiene como propósito realizar un análisis forense apoyados en la norma PCI-DSS a la red LAN de la Universidad Tecnológica Equinoccial UTE, para detectar información involucrada en los pagos de tarjeta de crédito que realizan las personas sobre los servicios que brinda la Universidad a la sociedad, determinando cuales son los riesgos y amenazas a los que se encuentra expuesto el usuario, y el impacto que se puede producir en el caso de que llegara a suceder estos eventos.

Para ejecutar estas acciones se utilizará herramientas manuales o automatizadas como expone la norma PCI-DSS y, basándonos en las mejores prácticas para el análisis forense a redes de datos. De los resultados obtenidos se generan informes con planes de acción que contienen estrategias de protección preventivas, correctivas y detectivas para mitigar el impacto de los riesgos basadas en las mismas normas.

Con esto se generarán políticas de seguridad de la información con el objetivo de preservar las características de disponibilidad, integridad y confidencialidad.

2. METODOLOGIA

La metodología a aplicar dentro del desarrollo de este proyecto es experimental ya que se basa prácticamente en cuatro elementos claves que de acuerdo a lo que expone las mejores prácticas del análisis forense son:

- La identificación de la evidencia

- La preservación de datos recolectados
- El análisis de la información
- La presentación de los resultados

De la información obtenida de un sistema de información, red y aplicación para determinar la fuente de un ataque que se haya encontrados en estos.

El análisis forense tiene como objetivo la aplicación de guías, estándares y procedimientos definidos con el fin de recolectar, comparar, analizar y evaluar información procedente de un sistema, apoyado siempre en herramientas técnicas.

El análisis forense tiene aplicación en muchos campos y situaciones, desde teniendo resultados para requerimientos legales hasta establecer políticas de seguridad hacia un incidente en una organización, de cualquier manera el objetivo principal que se sigue un proceso forense esta dado en 4 pasos[1] los cuales se presenta en la Ilustración 1.

Ilustración 1 Fases Análisis Forense

Identificación de la evidencia.- Llamamos identificación, al inicio de la investigación forense, en donde identifica información sobre un circunstancia en particular (puede ser de varias formas, mediante los sistemas de gestión de seguridad, mediante notificación directa, etc.), y hay una verificación de la misma, siendo importante probar las fuentes de información. Debe establecerse una línea de tiempo del evento y es importante saber lo que pasó en el momento de la adquisición de las pruebas. El escenario y sus circunstancias que se deben generar.

Preservación de los datos.- Una vez se han identificado los datos, lo que sigue es preservar los datos implicando a que se tenga que evaluar y extraer las más importante de información de los datos recolectados.

Análisis de la evidencia.- En esta fase, para el análisis de evidencias digitales, hay algunos procedimientos a seguir que dependen, en gran medida, del tipo de escenario

[1] National Institute of Standards and Technology NIST en "Guide to Integrating Forensic Techniques into Incident Response".

que fue diseñado antes, o del tipo de evidencia que se solicita. Algunos de los análisis que se pueden realizar son:

- Definición de una línea de tiempo; -Análisis de palabras clave
- Análisis de los encabezados de los archivos
- Análisis de los valores hash
- Análisis de la información oculta o borrada
- Análisis de Malware (por ejemplo, rootkits, troyanos, spyware, etc.)
- Análisis de los procesos
- Análisis de registros
- Análisis del sistema de registro

Elaboración de informes y conclusiones.- Por último, se elaboran los informes con los resultados de los análisis realizados. A fin de explicar, de la mejor manera posible, las pruebas obtenidas, y así apoyar el proceso de resolución.

3. DISEÑO E IMPLEMENTACION

3.1. PCI – DSS

El robo de identidad, fraudes y violaciones de seguridad informáticos son problemas que enfrentan los procesadores de pago, los comerciantes y proveedores de servicios en el entorno actual de procesamiento de tarjetas de crédito.

Es por eso que a partir del año 2005 las principales entidades emisoras de tarjetas de crédito integrado por American Express, Discover Financial Services, JCB International, Mastercard Worldwide y Visa Inc. toman medidas para mejorar la seguridad, como la instauración de un foro para definir estrategias comunes para evitar fraudes y perdidas de datos relacionados con tarjetas de crédito para lo cual creó el estándar Payment Card Industry – Data Security Standard (PCI-DSS) , el cual está dirigido a entidades bancarias, comerciantes y proveedores de servicios implicados en el procesamiento, almacenamiento y/o transmisión de datos de tarjetas de pago.

Este estándar es de cumplimiento obligatorio para las entidades a las cuales apliquen con la finalidad de reducir el fraude relacionado con tarjetas de crédito.

Para ello esta estándar definió un conjunto de 12 requisitos organizados en 6 principios u objetivos de control.

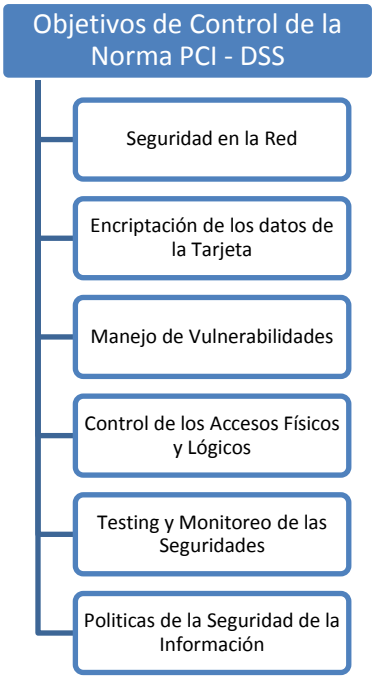

Ilustración 2 Objetivos de Control PCI-DSS

Desarrollar y mantener una red segura:

Requisito 1.- Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.

Requisito 2.- No usar contraseñas del sistema y otros parámetros de seguridad provistos por los proveedores.

Proteger los datos de la tarjeta habientes:

Requisito 3.- Proteger los datos almacenados de los propietarios de tarjetas.

Requisito 4.- Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.

Mantener un programa de gestión de vulnerabilidades:

Requisito 5.- Usar y actualizar regularmente un software antivirus.

Requisito 6.- Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar medidas solidas de control de acceso:

Requisito 7.- Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.

Requisito 8.- Asignar una identificación única a cada persona que tenga acceso a un computador.

Requisito 9.- Restringir el acceso físico a los datos de los propietarios de tarjetas.

Monitorear y probar regularmente las redes:

Requisito 10.- Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.

Requisito 11.- Probar regularmente los sistemas y procesos de seguridad.

Mantener políticas de seguridad de la información:

Requisito 12.- Mantener una política que contemple la seguridad de la información.

3.2. Captura de Paquetes

Es un software que ayuda a la captura de paquetes o tramas de una red para su posterior análisis.

Sus principales utilidades son las siguientes:

- Captura de contraseñas y nombres de usuarios en la red,
- Análisis de errores para descubrir problemas en la red,
- Medición del tráfico,
- Detección de intrusos, con la finalidad de descubrir hackers,
- Finalmente la de analizar la información en tiempo real que se transmite por la red.

4. RESULTADOS

4.1. Evaluación de Cumplimiento de la Norma

Como primera tarea fue analizar el estado actual de la institución de acuerdo a la norma PCI.-DSS. Para lo cual se realizaron entrevistas con los responsables de la administración de la red y personas de negocio de las áreas de tesorería y contabilidad, con los cuales se pudo identificar el proceso para la realización de pagos de los aranceles a través de tarjeta de crédito. Luego de acuerdo a las recomendaciones de la norma se realizó la segmentación de la red, para aislar aquellos elementos que procesan, almacena

o transmiten datos de tarjeta y definir los puntos en la red Lan donde se tomaron los datos con la herramienta OpenSource WireShark[2].

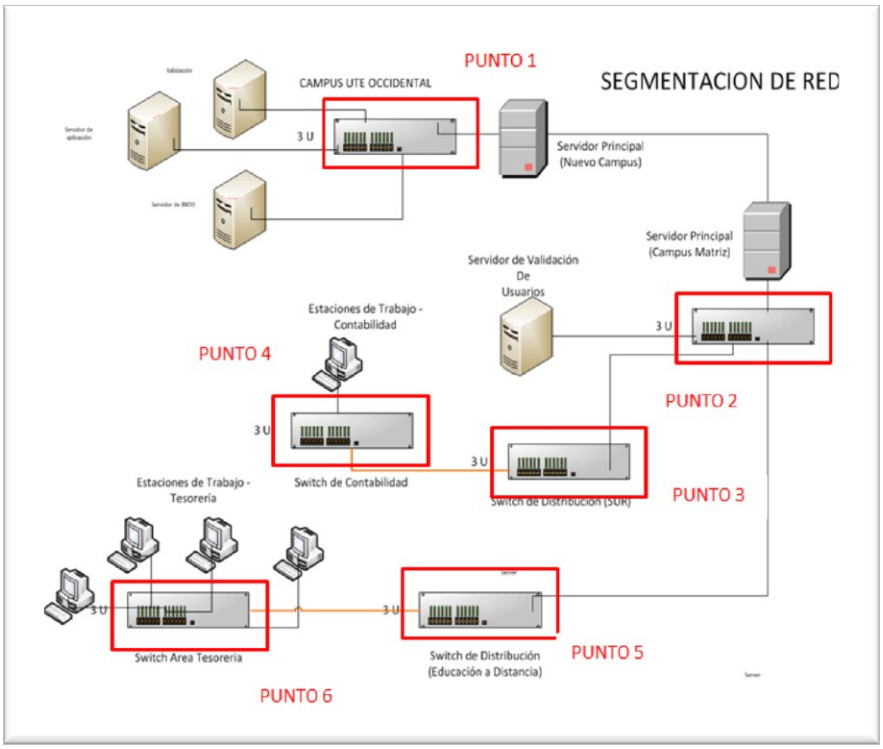

Ilustración 3 Segmentación de la Red

Luego de obtenidos los datos en los puntos indicados en la Ilustración 3 se procedió con el respectivo análisis para lo cual como primera herramienta se definió a WireShark ya que permite analizar los paquetes de datos de una red activa como también desde un archivo de lectura previamente generado mediante filtros, pero a través de la misma no se pudo obtener ningún resultado favorable.

Después se analizaron los archivos con el software OpenSource BreachProbe (Ilustración 4) que sirve para la realización de análisis forense

Al no encontrar ningún resultado con esta herramienta ni mediante filtros a través del WireShark se analizó las características del switch, en el que se identificó que el mismo divide los paquetes en diferentes tramas, ya que cada paquete es transportado por la red de forma independiente de los otros, paquetes pertenecientes al mismo mensaje puede viajar por caminos diferentes, de tal manera que la capa de transporte reordena los datagramas y recupera los paquetes perdidos, por lo que de manera manual ni con la herramienta BreachProbe se lograría encontrar los datos de número de tarjetas.

[2] WireShark Es una herramienta gráfica utilizada para analizar el tipo tráfico de una red en un momento determinado

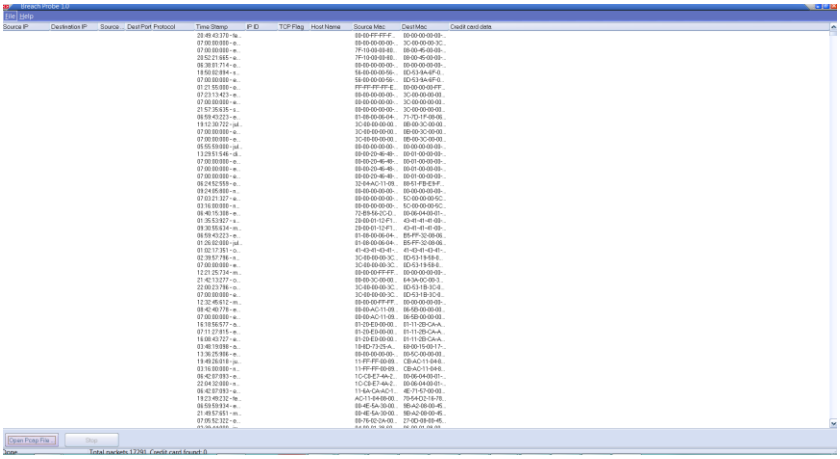

Ilustración 4 BreachProbe

Fuente: Software WireShark

Finalmente se investigó a la herramienta CCSRCH que de igual manera es un software libre, para lo cual a través de esta herramienta únicamente fue necesario dar el nombre del directorio y el archivo para que sea analizado y se encuentre números de tarjeta de crédito.

Es así que al analizar con esta herramienta los archivos obtenidos dentro del proceso de captura de datos se encontraron los resultados que se encuentran reflejados en las imágenes pero que por motivos de seguridad y de confidencialidad de los datos las imágenes se adulteraron las mismas para que el número de la tarjeta de crédito no sea legible por terceras personas dentro de este archivo. En la captura de datos del nodo del Área de Contabilidad (punto 4) se encontró una tarjeta de crédito con número 4303********4333 el mismo que puede visualizarse en la Ilustración 5.

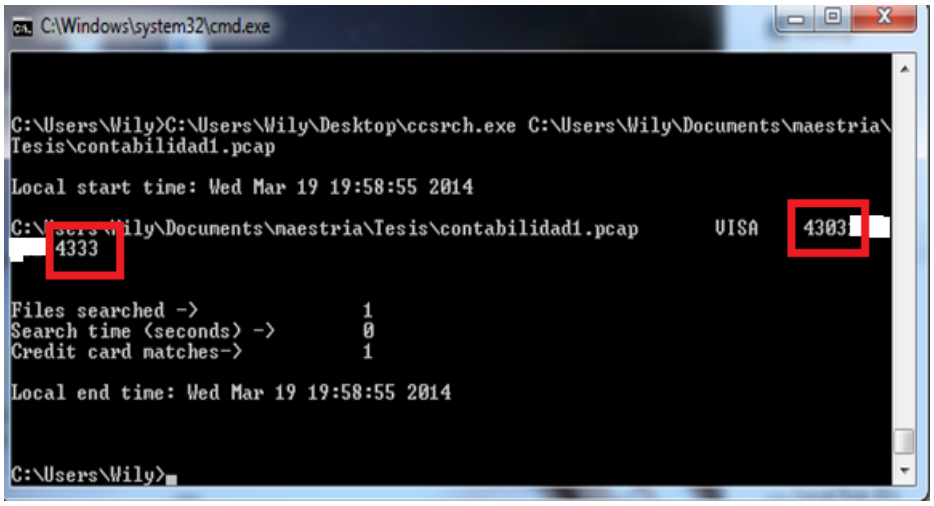

Ilustración 5 Contabilidad - CCSRCH Obtención Tarjetas de Crédito

Al cumplir el objetivo principal que es verificar que por la red Lan se transmiten números de tarjetas de crédito que no se encuentran cifrados o enciptados, se desarrolla proyectos en base a la necesidad de la institución de acuerdo a los requerimientos de la norma.

5. TRABAJOS RELACIONADOS

En el país existen instituciones financiaras certificadas con la norma PCI-DSS, sin embargo no existen entidades que controlen que los procesos de pago a través de tarjeta de crédito se realicen aplicando la norma.

Esta norma tiene la particularidad de fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

Es así que como proyectos futuros se propondría la implementación de evaluaciones a la Universidad Tecnológica Equinoccial de acuerdo a lo que dispone la norma PCI-DSS.

6. CONCLUSIONES Y TRABAJO FUTURO

El análisis forense realizado representa una solución preventiva para la seguridad de la información, y mediante las herramientas seleccionadas para este proyecto permitieron analizar los archivos de datos capturados en diferentes segmentos de la red, con lo cual se pudo identificar números de tarjetas de crédito, con lo que se determinó que el centro educativo no cuenta con un nivel adecuado de encriptación o cifrado que asegure la integridad y confidencialidad de los datos que se transmiten a través de su red.

Por tal motivo con la aplicación la norma internacional PCI-DSS la cual permite definir las medidas de protección para las infraestructuras de sistemas que intervienen en el tratamiento, procesamiento o almacenamiento de información de los medios de pago.

Finalmente con este proyecto se deja un plan de acciones a la universidad para ser implementado en el futuro, el cual le otorga un beneficio ya que asegura los datos del tarjeta habiente y previene los fraudes con tarjetas de crédito.

7. REFERENCIAS

LIBROS

[1.] Andrés E. León Zuluaga, T. E. (n.d.). *Guía metodológica para la investigación forense.*

[2.] Anton A. , C., & Branden R., W. (2012). *Understand and Implement Effective PCI Data Security Standard Compliance.* ELSEVIER.

[3.] Council, P. S. (2008). *Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) Exploración de PCI DSS.*

[4.] Gomez, D. R. (n.d.). Retrieved from Computo Forense Redes: http://cryptomex.org/SlidesForensia/ForensiaRedes.pdf

[5.] PCI QSA y ASV. (2009, Abril). *https://www.pcisecuritystandars.org/qsa_asv/index.shtml*.

[6.] PCI, P. C. (2012). *PCI Forensic Investigator (PFI).*

[7.] Pichirilo. (2013, Junio 03). *Indicios Digitales*. Retrieved from Análisis forense de la red. Una necesidad presente: http://indiciosdigitales.com/?p=1296

[8.] Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad, versión 2.0. (2010).

[9.] UTA. (n.d.). *http://repo.uta.edu.ec/handle/123456789/2895*. Retrieved from Universidad Técnica de Ambato: http://repo.uta.edu.ec/handle/123456789/2895