ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA A TRAVÉS DEL ANÁLISIS DE TRÁFICO EN REDES DE ÁREA LOCAL. APLICACIÓN A UN CASO DE ESTUDIO.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

ANDRÉS RODRIGO REINOSO CÓRDOVA
andres.reinoso@epn.edu.ec

Director: PhD. JENNY GABRIELA TORRES OLMEDO
jenny.torres@epn.edu.ec

Quito, Junio 2017

DECLARACIÓN

Yo, Andrés Rodrigo Reinoso Córdova, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Andrés Rodrigo Reinoso Córdova

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Andrés Rodrigo Reinoso Córdova, bajo mi supervisión.

_____

PhD. Jenny Gabriela Torres Olmedo
DIRECTOR

AGRADECIMIENTOS

Agradezco en primer lugar a Dios, por darme la capacidad, tenacidad, y fuerza para llegar hasta este punto de mi vida.

A mis padres y mi hermano, porque gracias a ellos soy la persona que soy.

A mis amigos, especialmente aquellos que siempre estuvieron ahí con sus palabras de aliento y cariño para que siga adelante, son muy importantes para mí.

A mis tíos, tías, primos y primas, y en general a toda mi familia porque son la mejor familia de todas.

A mi tutora, por su verdadero y constante apoyo durante el desarrollo de todo este trabajo.

A todas y cada una de las personas que me apoyaron de una u otra forma durante todo este periodo, de verdad se los agradezco.

DEDICATORIA

Para mis padres, mi hermano, mi familia, y todos mis amigos que aportaron en mi vida para que hoy pueda estar aquí, los quiero mucho.

ÍNDICE DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

El presente proyecto de titulación tiene como propósito realizar un análisis y evaluación de riesgos de seguridad informática a través del análisis de tráfico en redes de área local. Para la selección del marco de referencia para análisis y evaluación de riesgos, se realizó un análisis comparativo entre varios marcos de referencia reconocidos internacionalmente. El marco seleccionado de este análisis, sirvió de base para el desarrollo del modelo propuesto, en donde se identificaron seis fases para realizar la evaluación del riesgo. Para la selección de la herramienta de análisis de red, se realizó un proceso similar en donde se procedió a realizar un estudio comparativo de herramientas existentes para analizar el tráfico de red. De este análisis, se obtuvo la mejor herramienta la cual se utilizó en el proceso de evaluación de riesgos. El modelo propuesto consiste en realizar un match entre las fases determinadas para la evaluación de riesgos y la herramienta seleccionada. El modelo propuesto está basado en formularios los cuales son creados en cada fase del modelo propuesto, involucrando la herramienta determinada para el análisis del tráfico de la red. Estos formularios creados contienen las características y prácticas necesarias que se deben realizar en cada una de las fases de la evaluación del riesgo. Finalmente se procedió a la aplicación del modelo propuesto a un caso de estudio en un sistema de TI de una institución pública del Ecuador, en donde se analizó y evaluó exitosamente el riesgo validando así el modelo propuesto.

Palabras clave: Análisis y Evaluación de Riesgos. Análisis de Tráfico de Red LAN. Herramientas para el Análisis de Tráfico. Sistema de TI. Formularios para Evaluación de Riesgo.

ABSTRACT

The project aims to carry out an analysis and a risk assessment of computer security through the traffic analysis in local area networks. For the selection of the reference framework for risk analysis and assessment, a comparative analysis was carried out between several internationally recognized frames of reference. The selected framework for this analysis was the base to develop the proposed model, in which six phases were identified to carry out the risk assessment. For the selection of the network analysis tool, a similar process was performed in which a comparative study of existing network traffic analysis tools was carried out. From this analysis, the best tool was obtained which was used in the risk assessment process. The proposed model is based on a link between the phases determined for risk assessment and the selected tool. The proposed model is based on forms that are created in each phase of the proposed model, involving the determined network traffic analysis tool. These created forms contain the necessary practices and characteristics that must be developed in each phase of the risk assessment. Finally, the proposed model was applied to a case study in an IT system of a public institution in Ecuador, where the risk was analyzed and evaluated successfully, thus validating the proposed model.

Keywords: Risk Analysis and Assessment, LAN Network Traffic Analysis. Network Traffic Analysis Tools. IT System. Risk Assessment Forms.

1. INTRODUCCIÓN

Desde el establecimiento de la primera red de área local (LAN) comercial a finales del año 1977 en el Chase Manhattan Bank en la ciudad de New York [1], se ha avanzado hasta el punto de que en la actualidad se cuenta con millones de redes de área local en todo el mundo. Estas redes pueden ser desde un hogar de 3 o 2 nodos hasta grandes datacenters de 1000 nodos. Con esto han surgido numerosos problemas tanto a nivel físico, en la interconexión física de la red, como a nivel lógico, en la transmisión de la data a través de esta.

A nivel físico se han desarrollado normas internacionales como son la ANSI, ISO o IEEE para garantizar la calidad en los dispositivos y el correcto uso de los mismos [2], por ejemplo en la comunicación de red basada en la IEEE 802.3, se describe como debe ser el cableado mediante Ethernet, o el estándar ANSI/TIA/EIA-568 que es el encargado de definir la disposición de pines en la interfaz física de un RJ-45 o más comúnmente llamando cable UTP. A nivel lógico también se han desarrollado metodologías y estándares para gestionar riesgos en la transmisión segura de datos como por ejemplo el estándar ISO/IEC 27005:2011 [3] el cual nos proporciona directrices para la gestión de riesgos en la seguridad de la información en una organización, o el mismo IEEE 802.3 CSMA/CD que especifica un modelo de control de acceso al medio con funciones relacionadas al envío y recepción de datos [4]. Como se puede ver existen metodologías y estándares para el tratamiento de la red a nivel físico y lógico, entonces ¿cuál sería el problema?

A nivel físico se posee guías y un sinnúmero de tutoriales para la interconexión física de la red, de cómo montar una red de área local (LAN), con que dispositivos hacerlo, y como conectarlos; pero hay algo que necesita un mayor análisis y es poder evaluar los problemas que se generan en la red de área local. El problema se da para el administrador de una LAN que necesita obtener una respuesta práctica en torno a los riesgos que se generan en el tráfico de su LAN, también el usuario que pueda tener conceptos básicos de informática más no conozca metodologías para realizar un estudio profundo en la red y detectar las vulnerabilidades en la misma, administradores de redes LAN que necesiten un estudio de un coste bajo para identificar mal comportamientos en su red, detectar intrusiones no autorizadas, evaluar la sobrecarga que genera una aplicación, o simplemente analizar el tráfico existente en la red para obtener informes de rendimiento. Personas que al administrar una LAN,

identifiquen una sobrecarga en su red y no sepan cómo llevar un estudio de la misma para tratar esta clase de problemas. En síntesis, el problema se genera en torno a qué herramientas utilizar para dar solución a problemas generados en la red y que proceso o metodología seguir (de la gran cantidad existe) para realizar el análisis y evaluación de la red.

Es verdad que existen metodologías formales desarrolladas para lograr el objetivo principal, que sería gestionar el riesgo en la seguridad de la información, como la mencionada anteriormente ISO/IEC 27005:2011, o también existen varias herramientas para el análisis del tráfico de red que nos permiten desde capturar el tráfico hasta realizar un completo análisis de la misma como: ethercap, TCPdump, Wireshark, Colasoft Capsa entre otras. Pero para proveer una solución práctica para el problema planteado, se ha considerado que lo más óptimo es vincular los pasos claves en el análisis del riesgo, con una herramienta para realizar el análisis de tráfico, y todo esto presentarlo en formularios que optimicen el tiempo, a comparación de aplicar una metodología y realizar un análisis separado de la herramienta. Este análisis y evaluación del riesgo empezará proveyendo conceptos generales requeridos para el entendimiento del proyecto, después se realizará un análisis comparativo entre las marcos de referencia de análisis de riesgo y herramientas existentes para análisis del tráfico de red, se generará un match entre la herramienta seleccionada con las mejores prácticas resultantes del análisis comparativo de marcos de referencias seleccionados, y con esto se creará los formularios para la optimización de su aplicación, finalmente se aplicará el modelo propuesto a un caso de estudio.

2. MARCO TEÓRICO

2.1. Aspectos Generales de la Seguridad de la Información

En esta sección se define todo el sustento teórico relacionado con la seguridad de la información.

2.1.1. Activo

Un activo son los recursos del sistema de información o que están relacionados a él, los cuales son necesarios para que la organización funcione correctamente, y que además permiten que la organización alcance los objetivos propuestos [5].

2.1.2. Amenaza

Se considera como amenaza al potencial que tiene una fuente amenazante, evento o circunstancia para lograr explotar (accidental o intencionalmente) una vulnerabilidad específica, generando un efecto negativo en los activos de información de la organización o generando un impacto negativo a sus operaciones [6]. Las amenazas puedes ser de tipo naturales (terremotos, inundaciones, tormentas eléctricas, etc.), humanas, (entrada inadvertida a datos, actos no intencionales, ataques basados en redes, software maliciosos, etc.) y ambientales (polución, químicos, cortes de energía de larga duración, fugas de líquido) [7] [8].

2.1.3. Vulnerabilidad

Se define como vulnerabilidad al defecto o debilidad en un sistema de información, en los procedimientos de seguridad del sistema, controles internos, diseño, implementación o aplicación que puedan ser explotados (accidental o intencionalmente) y dan lugar a una infracción de seguridad o una violación de la política de seguridad del sistema [7] [8].

2.1.4. Impacto

El impacto hace referencia a la magnitud del daño que podría ser causado por una determinada fuente de amenaza una vez que explote una potencial vulnerabilidad [7]. El nivel de impacto se rige por los impactos potenciales de la amenaza, y a su vez produce un valor relativo para los activos de TI (Tecnología de la Información) y para los recursos afectados.

2.1.5. Riesgo

Se define como riesgo al impacto negativo neto del ejercicio de una amenaza, tomando en cuenta la probabilidad de ocurrencia como también el impacto a los procesos. La gestión de riesgos es el proceso de identificación y evaluación del riesgo, así como también la toma de medidas para reducir el riesgo a un nivel aceptable [7]. Por lo tanto se tiene que el riesgo es una función de probabilidad de que una determinada fuente de amenaza explote una potencial vulnerabilidad, y el resultante sea un efecto adverso a la organización [9].

2.1.6. Activo de Red

Un activo de red hace referencia a dispositivos o equipos físicos que permiten la conectividad de una o varias redes que pueden ser atacados intencionalmente o de forma accidental, generando problemas para el funcionamiento de la red y haciendo que esta no trabaje de forma óptima si estos activos son atacados [9].

2.1.7. Redes de Área Local (LAN)

Una red de área local (LAN) está limitadas por un espacio físico específico, generalmente de propiedad privada de una empresa, organización o incluso un domicilio. El interconectar equipos dentro de un área determinada dentro de las instalaciones físicas de una organización, compartiendo recursos e información y de esta manera facilitar el trabajo nos define lo que es una red de área local. Su principal objetivo es ofrecer a los usuarios la interconexión de nodos dentro de este tipo de red, acceso a internet, entre otros servicios específicos que involucran aspectos de telecomunicaciones como la telefonía. La tecnología LAN se ha desarrollado grandemente estos últimos años, llegando a manejar velocidades desde 1Gb hasta 10 Gb; generando un mínimo de error. Estas redes de área local actuales utilizan la familia de red Ethernet para su operatividad generalmente.

Una red de área local debe implementar características específicas para que mantengan una operatividad correcta, estas características son:

- **Escalabilidad:** la red debe tener la posibilidad de expandirse sobre sí misma o a nuevas redes, de acuerdo a las necesidades de la organización.
- **Administración:** las redes deben ser administradas, monitoreadas, analizadas para que en caso de algún desperfecto, se realice la respectiva corrección.
- **Costo-Beneficio:** se debe evaluar efectivamente si el costo de inversión es proporcional al beneficio que se obtendrá.

- **Alta disponibilidad:** la red debe estar disponible la mayor cantidad de tiempo posible.
- **Servicios:** la red debe soportar diferente tráfico, como datos, voz y video. Lo que requerirá una QoS (calidad del servicio).
- **Multiprotocolo:** la red debe permitir el uso de protocolos propietarios, ambientes con estándares y para diferentes fabricantes.
- **Movilidad:** la red implementa módulos con tecnología Wireless.
- **Seguridad:** la red debe proporcionar protección a los datos que se transfieren. Prevenir, mitigar y corregir los problemas que puedan presentarse.

2.2. ¿Qué es la Evaluación del Riesgo?

El proceso de evaluación del riesgo nos ayuda a determinar el alcance de una amenaza potencial sea externa o interna, y las vulnerabilidades en el sistema. [10]. Para esto se identifica la probabilidad y el impacto de que un evento pueda surgir de dichas amenazas o vulnerabilidades, definiendo funciones críticas necesarias para continuar con las operaciones regulares de una organización. Las amenazas en un sistema de TI deben ser analizadas en conjunto con las vulnerabilidades y controles establecidos para el sistema de TI con el objetivo de lograr evaluar el impacto.

El proceso de evaluación del riesgo involucra pasos esenciales los cuales globalmente se pueden asociar en [11]: (1) identificación de la amenaza, (2) identificación de la vulnerabilidad, (3) determinación del riesgo los cuales se amplían en el siguiente capítulo. Existen también metodologías que involucran recomendaciones de control en torno a los riesgos encontrados, esto se analiza en el siguiente capítulo igualmente [12].

3. SELECCIÓN DE LA METODOLOGÍA DE EVALUACIÓN DE RIESGOS

Este capítulo abarca un análisis comparativo de las metodologías de análisis de riesgo. Se iniciará con un listado de los marcos de referencia con una descripción de las características que ofrece cada uno de ellos. Posteriormente se seleccionarán las mejores prácticas de cada una de ellas y con estas se conformará una metodología compuesta con la cual se realizará el análisis y evaluación del riesgo.

3.1. Análisis Comparativo de Marcos de Referencia

Para el proceso de evaluación de riesgo de la seguridad de la información existe una gran cantidad de marcos de referencia entre las cuales encontramos guías, metodologías y estándares existentes en la literatura. La Agencia Europea de Seguridad de las Redes y de la Información ENISA (European Network and Information Security Agency), nos brinda un listado con 40 marcos de referencia existentes para la evaluación de riesgo entre los cuales se destaca a los 7 más utilizados que los encontramos en la Tabla 3.1. Marcos de Referencia para evaluación de riesgos más utilizados [13] [14].

Tabla 3.1. Marcos de Referencia para evaluación de riesgos más utilizados

N.	Marco de Referencia
1	NIST 800-30
2	ISO/IEC27005
3	MAGERIT
4	OCTAVE
5	FAIR
6	TARA
7	EBIOS

Las metodologías para realizar el análisis comparativo fueron seleccionadas en base a la facilidad de obtener la documentación, el idioma en que se encuentra disponible, y la aplicabilidad del marco de referencia en el proceso de evaluación del riesgo de seguridad de la información. Otro de los criterios utilizados fue el número de citas de

las metodologías en diferentes trabajos, como podemos ver en la Tabla 3.2. Citación de Marcos de Referencia, existen tres metodologías que fueron mayormente citadas por cada uno de los autores con trabajos referentes a la gestión del riesgo como son: ENISA [13], Mohamed S. Saleh [15], Palaniappan Shamala [16], Mohamed Ghazouani [17], Amril Syalim [18], Juan Manuel Matalobos Veiga [19] y Diana Pacheco [20]. Estas metodologías son: NIST 800-30, OCTAVE, MAGERIT con resultados de 7, 4 y 7 citaciones respectivamente. Adicionalmente a esta selección, a continuación se justificará teóricamente la selección de estas metodologías.

Tabla 3.2. Citación de Marcos de Referencia

Marco de Referencia / Autor	NIST 800-30	ISO/IEC27005	MAGERIT	OCTAVE	FAIR	TARA	EBIOS
ENISA	X		X	X			X
Mohamed S. Saleh	X			X			
Palaniappan Shamala	X		X	X			
Mohamed Ghazouani	X	X		X			X
Amril Syalim	X						
Juan Manuel Matalobos Veiga	X	X	X	X	X		
Diana Pacheco	X		X	X			
TOTAL	**7**	2	**4**	**7**	1	0	2

3.2. Selección de la Metodología y Justificación

Con la selección de los marcos de referencia necesarios para realizar el análisis comparativo los cuales son: NIST SP800-30, MAGERIT y OCTAVE, se procederá a dar las características fundamentales, presentando las mejores prácticas (mejores fases) de cada una de ellas para obtener un marco de referencia asociado con el cual se trabajará posteriormente.

3.2.1. NIST SP800-30

El Instituto Nacional de estándares y tecnología (NIST), desarrollado por el departamento de comercio de los estados unidos, en su publicación 800-30 realizada el año 2002 y su posterior revisión en el 2012, ha definido una "Guía de gestión del riesgo para sistemas tecnológicos de información" posteriormente renombrada en la primera revisión con el nombre de "Seguridad de la Información", con el propósito de desarrollar un programa eficaz de gestión de riesgos, que contiene tanto las definiciones y la orientación práctica necesaria para evaluar y mitigar los riesgos identificados dentro de los sistemas

El proceso de evaluación del riesgo nos ayuda a determinar el alcance de la amenaza potencial y el riesgo asociado a un sistema de TI. Este proceso nos ayuda a identificar los controles apropiados que se deben tomar para reducir o controlar el riesgo durante el proceso de mitigación de riesgos. Las amenazas en un sistema de TI deben ser analizadas en conjunto con las vulnerabilidades y controles establecidos para el sistema de TI con el objetivo de lograr evaluar el impacto a lo cual se hará referencia en la sección de "evaluación del impacto" de este modelo. La metodología de evaluación de riesgos, comprende cuatro pasos principales según la segunda revisión de la NIST SP 800-30, los cuales son [6] [21]:

Paso 1: Preparación para la evaluación del riesgo: El propósito de esta sección es identificar el contexto en el cuál se realizará la evaluación del riesgo, lo que implica identificar: propósito, alcance, supuestos y limitaciones, fuentes de información e insumos requeridos, y el modelo de riesgo y enfoques analíticos, todo asociado a la evaluación del riesgo de un sistema de información.

Paso 2: Conducción de la evaluación del riesgo: El propósito de esta sección es producir una lista de riesgos en la seguridad de la información que pueden ser priorizados por el nivel de riesgo y usados para informar decisiones en respuesta al

mismo, esto incluye: identificar fuentes de amenazas relevantes a la organización, identificar eventos que pueden ser producidos por estas fuentes de amenaza, identificar vulnerabilidades dentro de la organización que podrían ser explotadas por fuentes de amenaza y sus variantes, identificar la probabilidad de que los eventos de amenaza tuvieran éxito, determinar el impacto adverso a las operaciones de una organización, y determinar los riesgos como una combinación de probabilidad de amenaza e impacto de la explotación.

Paso 3: Comunicar y compartir los resultados de la evaluación de riesgo: Esta sección se enfoca en comunicar los resultados de la evaluación del riesgo al personal de toma de decisiones dentro de la empresa para saber dar respuesta al riesgo, así como compartir información relacionada con el riesgo que ha sido generada durante el proceso de la evaluación.

Paso 4: Mantenimiento de la evaluación del riesgo: El objetivo de este paso es mantener actualizado la información específica acerca de la evaluación del riesgo en la organización. Esta práctica es esencial en la organización ya que permitirán tomar decisiones de gestión y orientan las respuestas de riesgo.

Las directrices establecidas en la NIST SP800-30 específicamente enfocados en la sección para la evaluación de riesgo en sistemas de información, encaja adecuadamente en el modelo procedimental planteado, ya que provee los pasos necesarios en la evaluación del riesgo los cuales son esenciales en el planteamiento del análisis y evaluación a realizarse, estas directrices brindan la información de qué realizar en cada paso y su vinculación con los pasos subsecuentes para dar tratamiento del riesgo, y permite acoplar efectivamente el tratamiento de los riesgos enfocados en la red de área local, lo que concierne a este modelo.

Finalmente las directrices establecidas en la NIST 800-30, permiten evaluar las amenazas en torno a su nivel de impacto en la organización, para así lograr su posterior mitigación en base al set de recomendaciones, generando la mitigación de los riesgos identificados.

3.2.2. OCTAVE

“OCTAVE Allegro” es un método de evaluación para determinar las necesidades de seguridad en una organización desarrollado por el CERT (Computer Emergency Response Team), una división del Instituto de Ingenieros de Software (SEI) de la

universidad Carnegie Mellon. OCTAVE Allegro está basado en dos métodos antiguos denominados “OCTAVE Original” y “OCTAVE-S”. El método OCTAVE se centra en los activos de información y permite a los equipos de TI y personal involucrado en el negocio lograr hacer frente a las necesidades de seguridad de la información en la organización, brindando un enfoque basado en los riesgos operativos de seguridad y enfocando a la tecnología en dirección de un contexto empresarial.

OCTAVE puede ser ejecutado en un entorno colaborativo, y es muy adecuado para las organizaciones que quieren llevar a cabo una evaluación de riesgos sin involucrar extensivamente a la organización [22]. OCTAVE Allegro consta de ocho pasos organizados en cuatro fases las cuales son [22] [23]:

Fase 1: Desarrollar criterios de medición de riesgo consistentes con la misión de la organización, el propósito de los objetivos, y los factores críticos de éxito.

- **Paso 1:** Establecer Criterios de Medición del Riesgo.

Se define un conjunto cualitativo de medidas (criterios de medición de riesgos) con las que podrá evaluar el efecto de un riesgo sobre la misión y los objetivos empresariales de la organización así como también priorizar las áreas de impacto de la más importante a la menos importante.

Fase 2: Crear un perfil de cada uno de los activos críticos de información, establecer límites claros para cada activo, identificar sus requisitos de seguridad, e identificar todos sus contenedores (dónde se está almacenando, procesando y transportando dicha información).

- **Paso 2:** Desarrollar un Perfil para el Activo de Información.

Consiste en identificar y recolectar información de los activos sobre los cuales se podría realizar una evaluación que se centrará en los activos más importantes para la organización, se debe identificar al propietario del activo, anotar los requisitos de confiabilidad, integridad y disponibilidad e identificar el requerimiento de seguridad más importante del activo.

- **Paso 3:** Identificar los Contenedores del Activo de la Información.

Se identifican y documentan los contenedores donde se encuentran almacenados, procesados y transportados los activos de información, además de documentar también el propietario de dicho contenedor.

Fase 3: Identificar las amenazas de cada activo de información en el contexto de sus contenedores.

Paso 4: Identificar Áreas de Interés.

Se revisan cada uno de los contenedores identificados en el paso 3 para determinar las áreas de interés en la organización, se documenta cada una de las áreas identificadas, y se enfoca en las áreas que puedan generar mayor preocupación en torno a un escenario de amenaza. Se crean escenarios de amenazas en torno a las áreas encontradas.

- **Paso 5:** Identificar Escenarios de Amenazas.

Se identifican escenarios de amenazas que no se encuentran en áreas de interés, pudiendo si se requiere agregar probabilidad a cada uno de los escenarios identificados y logrando así determinar cuál de los escenarios es más probable de que ocurra.

Fase 4: Identificar y analizar los riesgos para los activos de información y empezar a desarrollar enfoques de mitigación.

- **Paso 6:** Identificar Riesgos.

Se determina el impacto de un escenario de amenaza en una organización, es decir, las consecuencias generadas por el impacto. Se documenta las consecuencias siendo los más específico posible.

- **Paso 7:** Analizar Riesgos.

Se evalúa las consecuencias de cada una de las áreas de impacto y se registra un valor de “alto”, “medio” o “bajo” para la organización. Estas consecuencias señalan efectos directos en la reputación de la organización, pérdidas monetarias potenciales y posibles demandas a la organización.

- **Paso 8:** Seleccionar un Enfoque de Mitigación.

Se clasifica cada uno de los riesgos según su puntaje para facilitar la posterior toma de decisiones en la cual se asigna un enfoque de mitigación para cada uno de los riesgos detectados mediante una estrategia elaborada.

La metodología que nos brinda OCTAVE provee instrucciones detalladas en cuatro secciones que involucran ocho pasos para realizar una evaluación del riesgo en sistemas de información a lo cual está enfocado el modelo procedimental planteado. Al ser una metodología detallada y con documentación disponible, además de que no requiere que la organización se involucre extensivamente, permite acoplarla adecuadamente al análisis comparativo que se realizará posteriormente [22] [23].

3.2.3. Magerit

Magerit V3.0 es creada por el Consejo Superior de Administración Electrónica (CSAE) como “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, con el propósito de establecer principios para el uso eficaz, eficiente y aceptable de las TI (Tecnologías de la Información), y garantizando el equilibrio de riesgos y oportunidades derivado de su uso [9]. La metodología Magerit establece dos grandes pasos esenciales en el proceso de gestión del riesgo [9] [5] [24]:

Paso 1: Análisis de riesgos: En esta tarea se determina qué posee la organización a su disposición, y se trata de estimar qué posibles eventos podrían ocurrir. Para esta tarea se tiene los siguientes elementos:

- Activos: Son los elementos en el sistema de información (o estrechamente relacionado a él), que de una manera directa o indirecta son de valor para la organización.
- Amenazas: Son los incidentes que pueden causar algún impacto en los activos y por ende a la organización.
- Salvaguardas o contramedidas: Son los elementos de defensa o protección desplegados para que las amenazas no causen gran daño para la organización.

Con estos elementos se estima el impacto (lo que podría llegar a pasar) y el riesgo (lo que probablemente pase), con lo cual se puede llegar a conclusiones con fundamento y proceder a la fase de tratamiento del riesgo.

Paso 2: Tratamiento del Riesgo: Permite establecer un plan de defensa prudente con el cual se pueda defender a la organización contra incidentes que la puedan poner en peligro, y a su vez prepararla para contrarrestar emergencias, sobrevivir incidentes, y continuar operando bajo las mejores condiciones posibles; en este punto, el riesgo es reducido a niveles residuales que son asumidos por la organización.

Magerit establece pasos esenciales para la gestión de la seguridad en base a la evaluación del riesgo mediante lo cual permite reconocer los elementos de valor de una organización y determinar la mejor manera de proteger dicho elemento. Este marco de trabajo presentado por Magerit va acorde al análisis y evaluación de riesgo propuesto por lo cual es totalmente aplicable. [9].

3.3. Selección de la Metodología

En base a los marcos de referencia seleccionados (NIST SP800-30, OCTAVE Allegro, Magerit V3.0), en la Tabla 3.3. Análisis Comparativo de Marcos de Referencia para análisis de riesgo, se realiza un análisis comparativo basándose en las fases del análisis de riesgo y los criterios para la evaluación del riesgo que maneja cada uno de los marcos de referencia, los cuales fueron mencionados en la Sección 3.2 [20] [6] [5] [25] [11].

Tabla 3.3. Análisis Comparativo de Marcos de Referencia para análisis de riesgo

MARCOS DE REFERENCIA / FASES	NIST SP 800-30	OCTAVE ALLEGRO	MAGERIT V3.0
Caracterización del Sistema	X	X	X
Identificación de la amenaza	X	X	X
Identificación de la vulnerabilidad.	X	X	
Análisis de control	X	X	X
Determinación de la probabilidad	X	X	X
Análisis de impacto	X	X	X
Determinación del riesgo	X	X	X
Recomendaciones de control	X	X	
Documentación resultante	X		
Establecimiento de parámetros		X	X
Necesidades de seguridad			X

En base al contenido de la Tabla 3.3. Análisis Comparativo de Marcos de Referencia para análisis de riesgo, se concluye que las mejores prácticas del análisis y la evaluación del riesgo son las fases en las que los tres marcos de referencia se involucran los cuales son:

- Caracterización del sistema
- Identificación de la amenaza
- Análisis de control
- Determinación de la probabilidad
- Análisis de Impacto
- Determinación del Riesgo

Con estas prácticas es posible realizar una vinculación con las herramientas propuestas en el Capítulo 4 y realizar el respectivo análisis y evaluación de riesgo en la red que se abarca en el Capítulo 5.

4. SELECCIÓN DE LAS HERRAMIENTAS PARA LA DETECCIÓN DE AMENAZAS Y VULNERABILIDADES MEDIANTE EL ANÁLISIS DE TRÁFICO DE RED

4.1. Análisis de Tráfico de Red

Análisis de tráfico de red es un proceso mediante el cual se graba, revisa y analiza el tráfico de red con el propósito de mejorar el rendimiento, la seguridad o realizar operaciones generales de mantenimiento en la red [7]. Este proceso involucra técnicas manuales o automáticas para revisar detalles a un profundo nivel y poder brindar estadísticas en torno al tráfico de la red.

Este análisis de tráfico de red se lo realiza para identificar paquetes sospechosos o maliciosos dentro del tráfico. Del mismo modo, un administrador de red utiliza este proceso para monitorear la velocidad de subida y bajada de datos, rendimiento de la red, contenido que fluye en la misma y para la comprensión de las operaciones realizadas en la red. Incluso el análisis del tráfico de red es utilizado por los mismos atacantes para encontrar patrones de tráfico o cualquier vulnerabilidad que pueda ser explotada [7].

De manera muy general, una herramienta para análisis de tráfico de red está compuesta principalmente de 5 partes [26]:

1. **Hardware:** La mayoría de los analizadores de tráfico red están basados en software y trabajan con sistemas operativos estándar (SO) y tarjetas de interfaz de red (NIC). Sin embargo, hay algunos analizadores de red de hardware especiales que ofrecen beneficios adicionales como el análisis de fallas de hardware incluyendo: Errores de redundancia cíclica (CRC), problemas de voltaje, problemas de cable, jitter (fluctuaciones en el envío de señales digitales), errores de negociación, etc.

   Algunos analizadores de red sólo soportan adaptadores de red inalámbricos o Ethernet, mientras que otras herramientas permiten el manejo de varias interfaces y personalizar su configuración.

2. **Controlador de captura:** Esta es la parte de un analizador de red que es responsable realmente de capturar el tráfico de red sin procesar desde el cable. Filtra también el tráfico de nuestro interés, y almacenar los datos en un buffer que es el núcleo principal de una herramienta para capturar tráfico.
3. **Buffer:** Este componente almacena los datos capturados. Los datos se pueden almacenar en un buffer hasta que esté lleno, o en un método de rotación "round robin", donde los datos más recientes reemplazan a los datos más antiguos.
4. **Análisis en tiempo real:** Esta función analiza los datos a medida que salen del cable. Algunos analizadores de red utilizan este método para encontrar problemas en el rendimiento y detectar intrusiones en la red.
5. **Decode:** Este componente muestra el contenido del tráfico de red con descripciones para que sea legible por el ser humano. Los decodes son específicos para cada protocolo, de modo que los analizadores de red tienden a variar en la cantidad de decodes que soportan.

Para determinar el proceso de análisis de tráfico de una red se hará referencia a un caso típico de análisis de tráfico de red validado por Laura Chappell [27] investigadora y fundadora de la Wireshark University [28] y de la Chappell University [29]. En este caso, un cliente empezó a notar un actuar extraño en su sistema, desde un rendimiento lento hasta la incapacidad de poner su equipo en hibernación o incluso de apagarlo [27]. El administrador de red se enfocó en la captura de tráfico para determinar la causa del porqué de este comportamiento extraño, y para la resolución del mismo se plantearon 4 pasos esenciales en el análisis del tráfico de red:

1. **Plan de análisis:** La persona encargada de determinar el problema empezó el proceso de análisis con la evidencia brindada por el usuario, por lo cual se decidió en primer lugar capturar el tráfico cerca del host que contenía los problemas para determinar si existía algún tráfico inusual desde o hacia el mismo. Con un conocimiento previo de qué protocolos maneja este host, se decide no instalar Wireshark en el host, ya que este puede estar infectado con algo que genere el problema, siempre es mejor ser discreto durante el proceso de captura, por lo cual se conecta un "tap de red" full dúplex (que deja pasar los datos en ambas direcciones) y conectar a su vez el Wireshark a este tap. Finalmente se configura el Wireshark en modo oculto.

2. **Captura:** Se empieza el proceso de captura sin ningún filtro para poder observar todos los paquetes de o hacia el host. Observando el tráfico durante la captura, se empieza a observar una enorme cantidad de paquetes TCP SYN (utilizados para establecer una conexión con el servidor) hacia el puerto 135 (puerto de servicio de sesión de NetBios), y hacia el puerto 445 (Servicio de Directorio de NetBios). También se observa que existe algún tráfico ICMP (generalmente usado para saber si un host está disponible). Mientras la captura de tráfico sigue, el administrador de la red empieza con el análisis.

3. **Análisis:** En el tráfico se observa conexiones hacia un servidor inusual (TCP puerto 18067), por lo que siguiendo esta trama TCP, se identificó algunos comandos usados en IRC (Internet Relay Chat - protocolo para comunicación parecido al chat que no requiere una conexión previa entre los usuarios y es orientado a grandes grupos de usuarios en lugar de conexiones uno a uno. [30]). Y en un análisis más detallado se observó que estos comandos IRC estaban usando métodos para evadir detecciones de reglas de IDS o firewall. Este hecho de que se estaban ejecutando estos comandos y de que existía una evasión al firewall del sistema, además de que se estaba haciendo una conexión a un puerto IRC que no maneja el estándar. Indica que el programa generado estaba siendo astuto. Un análisis más detallado nos permite observar que el canal utilizado por el IRC estaba siendo utilizado para descargar una aplicación maliciosa. Además se pudo identificar el nombre del host del servidor IRC. Se concluyó entonces que el host de en el análisis estaba infectado con algo. Entonces utilizando toda la evidencia disponible obtenida: nombre de host, nombre de archivo descargado, número de puerto utilizado, etc. Se supo concluir que se estaba enfrentándonos a un bot (programa informático que trata de simular el comportamiento humano). Además se pudo identificar cuál fue el fallo de seguridad que causó esta intromisión en el host, y en muchos otros de la red para volverla vulnerable.

4. **Documentación:** El analista de redes documenta todos los hallazgos y su proceso para educar a: los usuarios en torno a los síntomas experimentados, al gestor de la red para estar pendiente en torno a futuras vulnerabilidades y al resto de personal de TI en torno al procedimiento que se debe realizar para la limpieza de la red. Posterior a esto en el proceso de “limpieza de la red”, se realizará un paso denominado “aseguramiento” donde se eliminará la amenaza y vulnerabilidad documentada en el proceso de documentación. Se cierra entonces el caso

generado en este escenario con problemas de seguridad, con lo cual se abarcó las cuatro fases del análisis de tráfico de la red.

Este proceso de análisis de tráfico de red generalmente se lo realiza mediante software utilitario específico para esta tarea, llamados *sniffers* de red. Existe una gran cantidad de sniffers de red unos con más utilidades que otros pero en general todos nos permiten el objetivo de poder analizar el tráfico de una red.

4.2. Herramientas para Análisis Comparativo

En esta sección se presentan varias herramientas para análisis de tráfico de red, se realizará un análisis comparativo de herramientas, y posteriormente se seleccionará la mejor herramienta con la cual se realizará el análisis. Actualmente existe una gran cantidad de herramientas para el análisis de tráfico en la red como se puede visualizar en la Tabla 4.1. Sniffers de Red Existentes, estas herramientas son las más referenciadas por los autores: Sumit Dhar [31], Jhilam Biswas [32], Ryan Spangler [33], Charu Gandhi [34], Andrew Tabona [35], Jack Wallen [36], Roger Grimes [37], Ishan Bansal [38], Cert [39], Elseiver [40], Ankit Gupta [41].

Tabla 4.1. Sniffers de Red Existentes

Autor / Herramienta	Sumit Dhar	Jhilam Biswas	Ryan Spangler	Charu Gandhi	Andrew Tabona	Jack Wallen	Roger Grimes	Ishan Bansal	Cert	Elseiver	Ankit Gupta
TCPdump	X			X				X	X	X	
Sniffit	X										
Etherreal	X						X				
Hunt	X										
Ettercap	X									X	
Dsniff										X	
SmartSniff											X
Wireshark		X		X	X	X		X	X	X	X
Capsa				X	X			X		X	

Fiddler					X						
Microsoft Network Monitor					X			X			X
NAST						X					
Zenmap						X					
EtherPeek										X	
AntiSniff			X								

Como se puede evidenciar en la Tabla 4.1. Sniffers de Red Existentes, las herramientas más utilizadas son Wireshark con 8 referencias, TCPdump con 5 referencias y Capsa con 4 referencias las cuales se detallarán a continuación.

4.3. Análisis Comparativo y Selección de la Herramienta

Una vez justificada la selección de las herramientas de análisis de red necesarias para realizar el análisis comparativo, los cuales son: Wireshark, TCPdump y Capsa Packet Sniffer, se procederá a dar las características fundamentales, presentando las mejores prácticas de cada una de ellas para obtener la herramienta con la cual se trabajará posteriormente.

4.3.1. Wireshark

Wireshark es el analizador de protocolos de red más importante en todo el mundo, permite observar lo que está ocurriendo en la red a un nivel microscópico. Incluso en muchas empresas e instituciones educativas es considerado como un estándar de facto. [34] [38] [39] [42]. Este software open source, prospera cada vez más con la ayuda de todos los expertos de redes en el mundo, un proyecto que empezó en 1998.

Es utilizado para analizar la estructura de diferentes protocolos de red y tiene la habilidad de demostrar la encapsulación que realiza TCP/IP. Este software puede operar sobre sistemas operativos Unix, Linux y Windows e implementa los complementos GTK+ y PCAP para la captura de los paquetes; está basado en la licencia pública general GNU.

Wireshark soporta una interfaz gráfica de usuario con características de filtrado de información con lo cual permite observar todo el tráfico que se transmite por la red [43] [27]; como se puede observar en la Figura 4.1. Interfaz Gráfica de Wireshark. Entre sus características principales se tiene [39] [43]:

- Los datos pueden ser analizados ya sea en el instante en que se transmiten sobre la conexión de red o desde archivos que contienen paquetes de datos ya capturados.
- Involucra un módulo de línea de comandos llamada Tshark.
- Admiten lectura de datos en tiempo real para una amplia gama de redes y protocolos (Ethernet, IEEE 802.11, protocolo punto a punto, loopback o protocolos de retorno).
- Mediante la interfaz gráfica se puede navegar a través de los datos de red capturados.
- Maneja un licenciamiento GNU y no posee ningún costo.
- Presenta una interfaz gráfica intuitiva y de fácil manejo.
- Trabaja con más de 1100 protocolos en su análisis de tráfico.
- Soporta tráfico de voz IP, y si es capturado correctamente incluso puede ser reproducido.
- Soporta los sistemas operativos Linux, Windows y Mac.

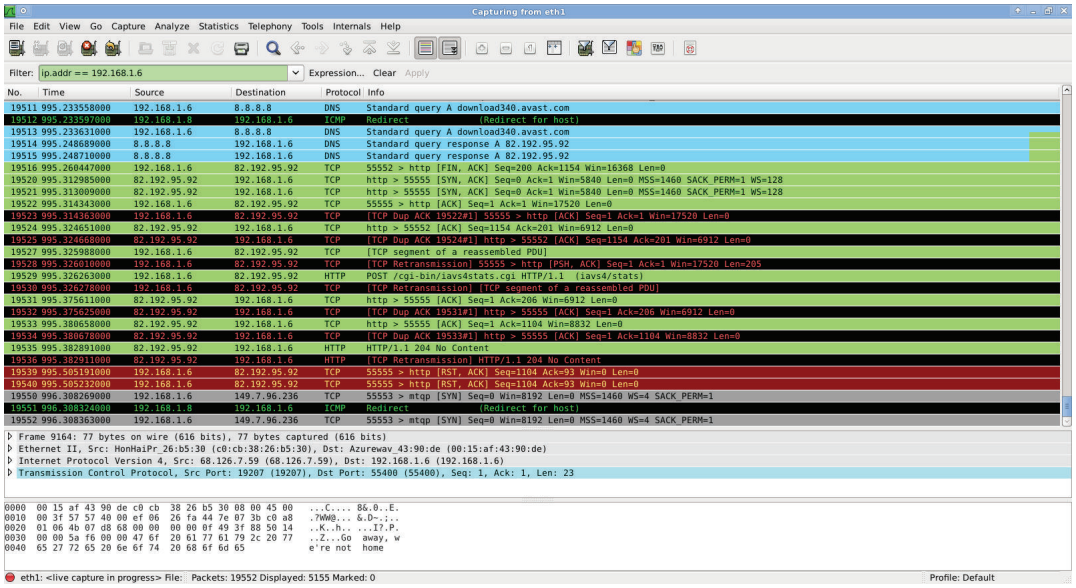


Figura 4.1. Interfaz Gráfica de Wireshark

4.3.2. TCPDump

Es una herramienta creada por: Van Jacobson, Craig Leres y Steven McCanne, utilizada para la captura de paquetes, monitoreo de red y depuración de protocolos. Es la línea de comandos más antigua y más comúnmente utilizada. Únicamente estaba disponible en los sistemas operativos Linux, pero actualmente también existen compilaciones de la versión original de Linux para Windows [34] [38] [44] [45].

Al finalizar un análisis con TCPdump, este se detiene y muestra el número de paquetes capturados y el número de paquetes descartados. La ventaja principal de TCPdump sobre otros sniffers de paquetes es que se puede utilizar de forma remota con la menor sobrecarga y por lo tanto, preferido por aquellos administradores que les gusta trabajar desde una red diferente. Entre sus principales características se tiene:

- Es la herramienta más difundida y utilizada para en análisis de la red.
- Existe en versiones portables por el tamaño reducido de la aplicación.
- No posee una interfaz gráfica por lo que provee un alto rendimiento en la captura de tráfico.
- Es un software de código abierto que puede ser utilizado para leer la captura en vivo o un archivo de captura ya creado.
- Se puede ejecutar remotamente mediante el inicio de sesión de Telnet o SSH.
- Soporta varias interfaces de red como son: Ethernet, Token-ring, FDDI, WIC.
- Captura datos en formatos libpcap, que es utilizado en la mayoría de las herramientas
- Es un software gratuito para sistemas operativos Linux y de pago para Windows, aunque para este último posee una versión de prueba.

Un ejemplo de la interfaz se puede visualizar en la Figura 4.2. Interfaz de TCPdump para Windows.

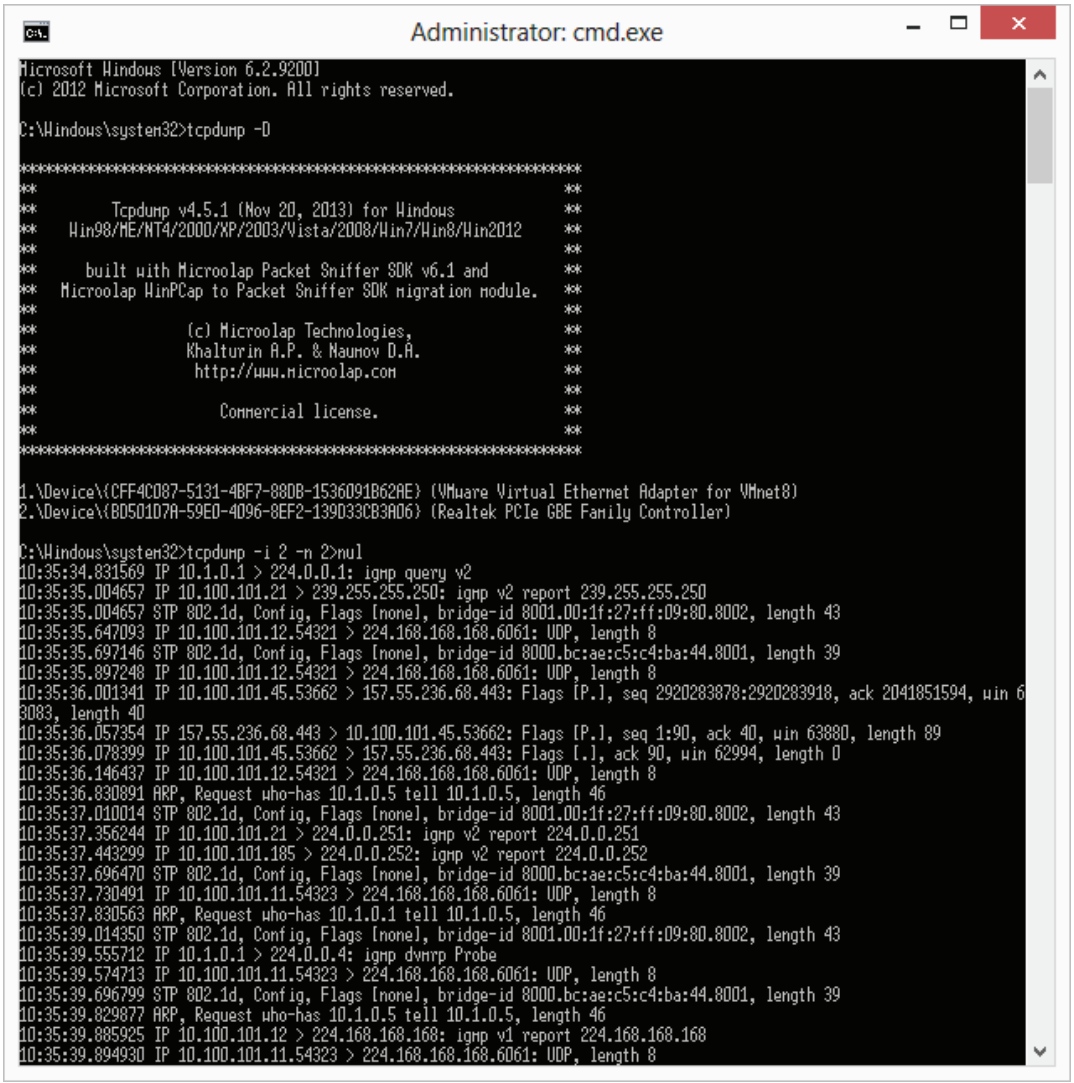


Figura 4.2. Interfaz de TCPdump para Windows

4.3.3. Capsa Packet Sniffer

Capsa es un sniffer de red muy completo de la empresa Colasoft para análisis de paquetes de tráfico de red, este software viene en versión gratuita y en versión de pago. La versión gratuita posee varias características y es lo suficientemente bueno para el uso doméstico así como también para pequeñas empresas. Capsa realiza un análisis efectivo de la red en tiempo real, chequeando paquetes de red y analizándolos [34] [38]. La versión gratuita de Capsa permite monitorear 50 direcciones IP juntas, lo que hace que este sniffer de paquetes gratis sea especialmente útil para los administradores de red [38] [46]. A continuación se presentan algunas características de Capsa:

- Monitoreo detallado de todo el tráfico del ancho de banda de todos los ordenadores de la red.
- Diagnóstico de la red para identificar problemas.
- Registro de actividades de la red (registro de mensajes instantáneos y correo web).
- Supervisión del comportamiento de la red.
- Gracias a su interfaz gráfica, incluye su propio tablero de instrumentos que incluyen parámetros importantes y gráficos de análisis de red.
- Identifica y analiza más de 300 protocolos de red.
- Mejora y personalización de informes.
- Es un software propietario y su licencia tiene costo, aunque existe una versión gratuita limitada.
- Solo soporta sistemas operativos Windows e interfaces ethernet.

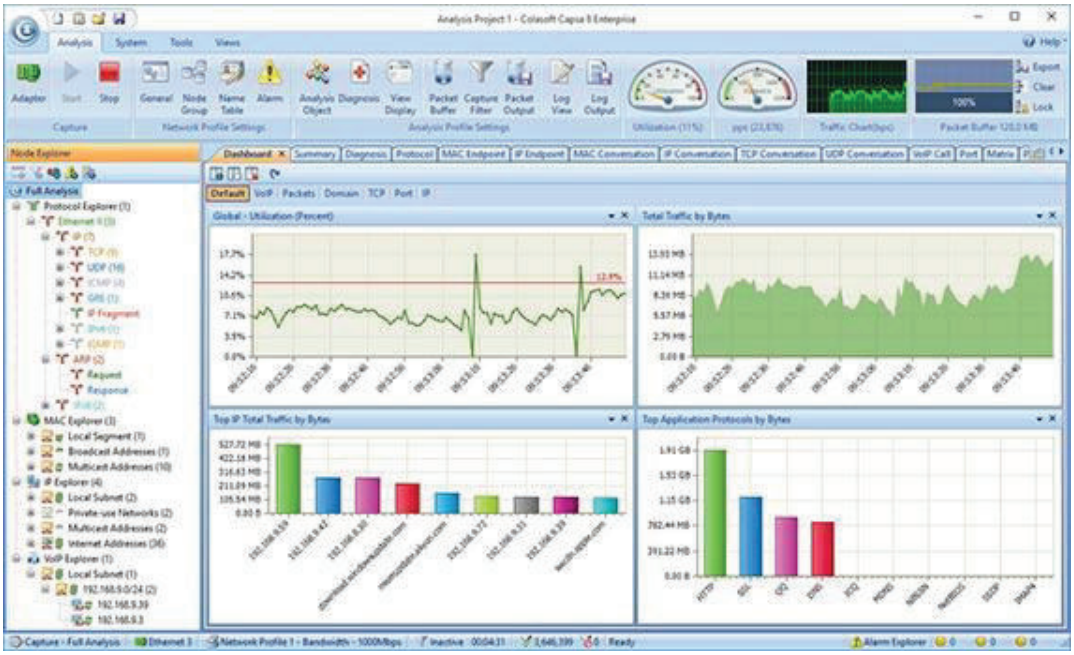


Figura 4.3. Interfaz gráfica de Capsa

4.4. Selección de la Herramienta

En esta sección se presenta un análisis comparativo en base a las herramientas para análisis de tráfico de red seleccionadas: TCPdump, Wireshark y Capsa. Los criterios seleccionados corresponden a las principales características de un sniffer de red, la

facilidad de obtención de la herramienta, licenciamiento, entre otras características; todo esto realizado en la Sección 4.3 [45] [44] [46] [43] [34].

Este análisis comparativo brindará un enfoque más claro en torno a la selección de la herramienta más adecuada para realizar el análisis del tráfico de red correspondiente necesario para este análisis metodológico.

Tabla 4.2. Tabla comparativa de sniffers de red

Herramienta / Características	TCPdump	Wireshark	Capsa	Herramienta(s) Seleccionada(s)	Criterio de selección
S.O. Soportado	Linux, Windows	Linux, Windows, MacOS	Windows	Wireshark	La herramienta se acopla a cualquier sistema operativo.
Última versión disponible	Última versión 4.9.0.	Última versión 2.2.5	Última versión 9.2.	Capsa	Mayor cantidad de versiones en el mercado y soporte para cada una de ellas.
Tamaño del aplicativo	Linux - 1231 KB Windows – 554.2KB	Windows - 47.1 MB MacOS - 31.3 MB Linux – 30.8 MB	Windows - 62.8 MB	TCPdump	Aplicativo de menor tamaño.
Costo	Gratuito - Linux $239.95 - Windows	Gratuito	$0 –Versión Gratuita $1000 – Versión Pago	Wireshark	Herramienta libre de fácil adquisición que no posee costo para ninguna de sus versiones.
Licenciamiento	BSD License	GNU / GPL	Freeware y Comercial	TCPdump / Wireshark	Las versiones completas manejan licenciamiento público de libre acceso al código fuente.
Interfaz gráfica de usuario	NO	SI	SI	Wireshark / Capsa	Herramientas que proveen interfaz gráfica para una mayor facilidad en el manejo.
Interfaz de línea de comandos	SI	SI	NO	Wireshark / TCPdump	Herramientas que permiten el manejo mediante terminal.

Protocolos Soportados	Aprox. 300	Más de 1000	Aprox. 300	Wireshark	Mayor cantidad de protocolos manejados.
Alarmas para tráfico y protocolos	NO	NO	SI	Capsa	Única herramienta que me permite generar alertas en torno al tráfico de red.
Identificar protocolos anómalos	NO	NO (Genera alarmas)	SI	Wireshark / Capsa	A pesar de que Wireshark no identifica protocolos anómalos, nos brinda una alerta si detecta un protocolo no identificado por lo cual es válida la selección. Capsa identifica los protocolos desconocidos.
Interfaces de red	Ethernet, Token-ring, FDDI, WIC	Ethernet, 802.11, PPP	Ethernet	Wireshark	Para realizar un análisis de tráfico de red se requiere interfaces Ethernet y 802.11 ya que son las que más difundidas actualmente tanto en hogares como en empresas.

En base a la Tabla 4.2. Tabla comparativa de sniffers de red, se obtiene que “TCPdump” es seleccionada tres veces en base a los criterios de selección expuestos; Wireshark se selecciona ocho veces y Capsa se selecciona cuatro veces. Por concluyente la herramienta seleccionada que nos ayudará en el proceso de análisis y evaluación del riesgo será Wireshark. Cabe mencionar que el analizador de tráfico de red puede ser cualquier herramienta que se crea conveniente y no se debe sentirse atado a la herramienta que se ha obtenido.

5. MODELO PROPUESTO

En este capítulo se abarca el análisis y evaluación del riesgo de una red de área local en base a la metodología y herramienta seleccionada en las secciones anteriores. Se empezará describiendo todos los pasos necesarios para realizar un análisis del tráfico de red cuando esta se encuentra bajo un escenario de ataque, posteriormente se vinculará la metodología de evaluación del riesgo obtenida con los pasos para análisis de tráfico de red según corresponda con la metodología, se generarán formularios a partir de este match entre metodología de evaluación de riesgo y herramienta para análisis de tráfico se generarán los formularios finales para el análisis y evaluación de riesgo mediante el análisis del tráfico de red.

5.1. Descripción del Modelo Propuesto

El modelo propuesto abarca las mejores prácticas de las metodologías de análisis y evaluación de riesgo, los diferentes pasos para el análisis de la red y la herramienta de evaluación de amenazas y vulnerabilidades. En el análisis y evaluación del riesgo las fases que se obtuvieron del análisis comparativo de las diferentes metodologías son:

- Caracterización del sistema
- Identificación de la amenaza
- Análisis de control
- Determinación de la probabilidad
- Análisis del Impacto
- Determinación del riesgo

Estas fases deben coordinarse con los pasos para realizar el análisis en el tráfico de red, los cuales son:

- Plan de análisis
- Captura
- Análisis
- Documentación

A partir de los pasos seleccionados, se requiere realizar un match entre las fases de la metodología para el análisis y evaluación de riesgo, con los pasos para el análisis de tráfico de red, los cuales posteriormente se presentarán en formularios para el análisis y evaluación de riesgo. Este match entre las fases determinadas para la evaluación de riesgos y los

pasos para análisis de tráfico de red se puede visualizar en la Figura 5.1. Match entre fases para evaluación de riesgos y pasos para análisis de tráfico.

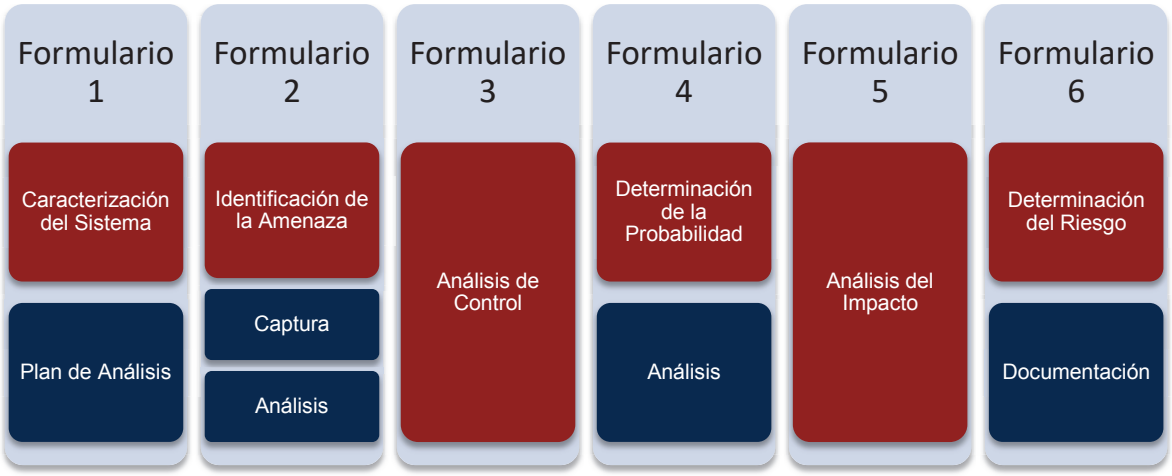


Figura 5.1. Match entre fases para evaluación de riesgos y pasos para análisis de tráfico

En la figura se puede observar cómo se estructura cada uno de los formularios para análisis y evaluación de riesgo, los cuales incluyen las fases de la metodología con los pasos para el análisis de tráfico de red. Posterior al análisis de tráfico de red se realiza también la fase llamada “aseguramiento” donde se trata la amenaza o vulnerabilidad encontrada en la red, este paso no consta en la figura ya que está fuera del proceso metodológico para el análisis y evaluación de riesgo y debería ser llevado a cabo por la organización posterior a la finalización de la aplicación metodológica en un plan de tratamiento del riesgo. El establecer un plan de tratamiento del riesgo, beneficiará a la organización en el proceso de mitigar el riesgo encontrado en los procesos manejados dentro de la organización pero esto hace parte de fases posteriores en la gestión del riesgo.

5.1.1. Caracterización del Sistema

Se debe recordar que en esta sección se identifican los límites del sistema de TI, junto con los recursos y la información que constituyen el sistema. La caracterización de un sistema de TI, establece el alcance del esfuerzo de la evaluación del riesgo y proporciona información (hardware, software, conectividad del sistema, división de apoyo o personal responsable) esencial para definir el riesgo. En este proceso de caracterización del sistema se describe la información relacionada con el sistema utilizado para caracterizar un sistema de TI y su entorno operativo y también las técnicas de recopilación de información que se pueden utilizar para solicitar la información pertinente para el entorno de ejecución del sistema de TI [11] [6] [21].

Se responderá a la pregunta ¿dónde realizar el análisis del tráfico de red? Esto dependerá del conocer el funcionamiento de la red, de cómo se encuentra estructurada, y los debidos accesos que se tiene a esta. En este punto se requiere vincular la herramienta para que nos ayude con la caracterización del sistema, para lo cual nos referiremos al paso de “plan de análisis” para el análisis del tráfico de red.

5.1.1.1. Plan de Análisis

Si la red de área local abarca un entorno en el cual ya se involucra un servidor y uno o varios switches, y por ejemplo se tiene el problema de que el rendimiento de la red ha disminuido considerablemente desconociendo la causa, entonces se debe colocar la herramienta en el servidor el cual abastece los servicios a la red. Sin embargo, hay casos en los que no se puede tener un acceso físico al servidor para instalar la herramienta, ya sea por su ubicación, motivos de seguridad, políticas del entorno, o por varias otras razones. Entonces, a continuación se ofrecen varias alternativas de donde realizar la captura para recopilar los datos necesarios para en análisis de la red [5] [11] [22].

5.1.1.1.1. Utilizando un Hub de Red

Tal vez una de las opciones más fáciles que se pueda deducir, es conectando el equipo disponible con Wireshark a uno de los puertos de algún switch, pero hay que recordar que el tráfico se transmite por segmentos de nodo a nodo entre equipos por lo que si se realiza esta acción, se estaría observando simplemente el tráfico que se transmite en el segmento entre el switch y el equipo, y ese no es el objetivo. Por lo cual se debe utilizar un hub de red y conectarlo en el mismo segmento de red donde

se encuentra el servidor, para con esto lograr que el tráfico entre el servidor y el switch pueda ser alcanzado en el equipo con la herramienta [47]. La forma de esta conexión se puede observar en la Figura 5.2. Análisis de tráfico mediante Hub.

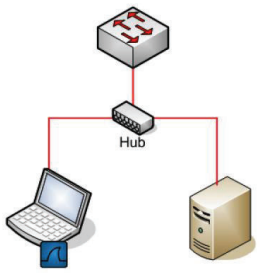


Figura 5.2. Análisis de tráfico mediante Hub

5.1.1.1.2. Utilizando Puerto Espejo (Port Mirroring)

Este método es uno de los más efectivos y fáciles de implementar para el análisis del tráfico de red. Consiste en duplicar el tráfico de red de uno o más puertos del switch en otro, este puerto por el cual se atravesará el tráfico de red duplicado tomará el nombre de puerto "mirror" el cual debe soportar velocidades iguales a las manejadas por el o los puertos los cuales se va a duplicar para evitar así perdidas de tramas [47]. La forma de conexión se puede visualizar en la Figura 5.3. Análisis de Tráfico mediante "Port Mirroring" [47].

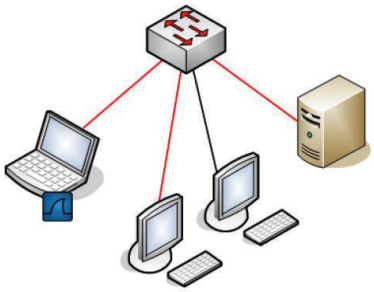


Figura 5.3. Análisis de Tráfico mediante "Port Mirroring"

En el siguiente ejemplo se observa cómo realizar esta acción en un switch Catalyst 2900XL/3500XL de Cisco [48].

Se desea configurar el puerto Fa0/1 como puerto de destino y los puertos de origen son el Fa0/2 y Fa0/5 además de que la interfaz de administración es la (VLAN 1), entonces se selecciona la interfaz Fa0/1 en el modo de configuración:

```
Switch(config)#interface fastethernet 0/1
```

Ahora se ingresa los puertos a ser monitoreados

```
Switch(config-if)#port monitor fastethernet 0/2
Switch(config-if)#port monitor fastethernet 0/5
```

Con este comando, todos los paquetes que estos dos puertos reciben o transmiten son copiados en el puerto Fa0/1. Ahora se debe emitir una variación del comando del puerto mirror con el fin de configurar el control para la interfaz administrativa:

```
Switch(config-if)#port monitor VLAN 1
```

Hay que tener en cuenta que este último comando no significa que el puerto Fa0/1 monitoree todo el tráfico de la VLAN 1. La palabra VLAN 1 se refiere simplemente a la interfaz administrativa del switch, es decir, con la interfaz que se va a monitorear.

Además se debe tomar en cuenta que no se puede configurar un puerto mirror fuera de la VLAN que contengan los puertos que se quieran duplicar, estos deben encontrarse en la misma VLAN.

5.1.1.1.3. Implementando Modo Bridge

Si no se tiene acceso al switch para realizar un port mirroring, se puede implementar un equipo que contenga dos tarjetas de red igualmente colocándonos entre el switch y el servidor, obteniendo así un acceso pasivo al tráfico que fluye entre estos dos nodos. La forma de conexión se observa en la Figura 5.4. Análisis de tráfico mediante “Modo Bridge [47].

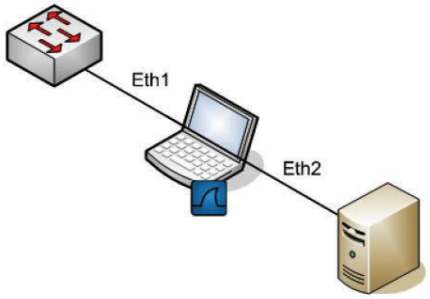


Figura 5.4. Análisis de tráfico mediante “Modo Bridge”

En Windows simplemente basta con seleccionar las tarjetas de red en la sección de “Conexiones de red” que se encuentra en el panel de control y mediante clic derecho se seleccione “Conexiones de puente” con lo que se creará una interfaz donde está realizado el puente de las dos tarjetas de red. [49] Esto se puede observar en la Figura 5.5. Conexión de Puente en Windows.

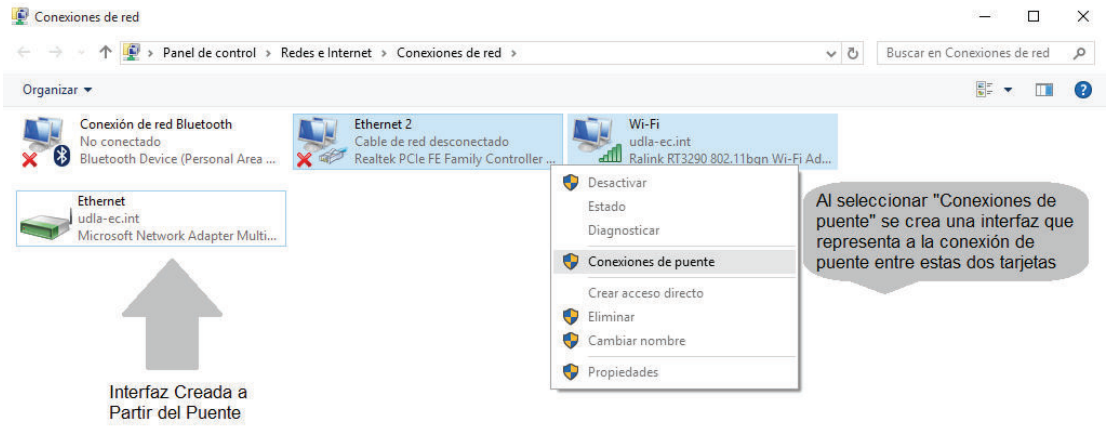


Figura 5.5. Conexión de Puente en Windows

En Linux de igual forma la creación del puente se la realiza de una forma sencilla mediante los bridge-utils ya que nos brindan una facilidad para la instalación y configuración. Simplemente se crea una interfaz “bridge” y se añaden las interfaces que se necesita que formen parte del puente. Finalmente se levanta esta interfaz y se ejecuta Wireshark [47]. Los comandos requeridos son los siguientes suponiendo que las tarjetas entre las cuales se requiere el puente son las eth0 y eth1:

```
root@areinoso:~# brctl addbr mybridge
root@areinoso:~# brctl addif mybridge eth1
```

```
root@areinoso:~# brctl addif mybridge eth0
root@areinoso:~# ifconfig mybridge up
```

5.1.1.1.4. Realizando un ARP Spoofing

Si no se puede implementar ninguna de las opciones mencionadas anteriormente, se puede valer de este método que puede ser considerado un poco agresivo para su implementación; este método generalmente es usado por atacantes para realizar una intromisión en la red. Herramientas como ettercap o la misma arpspoof nos permiten realizar un MitM (Man in the Middle), que es un método de intromisión en la red en el que el atacante se coloca en medio de una conversación, y se hace pasar por ambas partes obteniendo la información que las dos partes están tratando de enviar el uno al otro. Esta persona que se encuentra en el medio puede interceptar, enviar, recibir y hasta modificar en ciertas ocasiones la información de la una hacia la otra persona sin que las dos partes puedan darse cuenta [50].

Al realizar el “arp spoof” se logra que todas las tramas que se estén enviando en el segmento intervenido, pasen a través de la máquina donde se tiene Wireshark ejecutándose, esto se logra mediante una IP y una MAC falsa. Se tiene que tomar en cuenta de que si se implementa este método, existen switches con la capacidad de detectar intromisiones de este tipo por lo cual se debería desactivar esta opción de los dispositivos para que no exista ningún problema en la interfaz de conexión. Por ejemplo para interponernos entre el servidor (10.15.0.100) y la interfaz de LAN (10.15.0.1), tan solo se debe ejecutar ettercap con el comando:

```
root@areinoso:~# ettercap -T -M arp:remote /10.15.0.1/
/10.15.0.100/ &
```

Una ilustración de este método se puede encontrar en la Figura 5.6. Análisis de Tráfico mediante “Arp Spoof” [47].

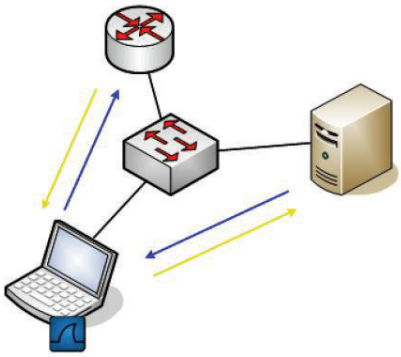


Figura 5.6. Análisis de Tráfico mediante “Arp Spoof”

5.1.1.1.5. Utilizando un TAP de red

Como se observó en la sección de activos de red, se puede implementar un tap de red para realizar el monitoreo de la misma, este tap al ser full dúplex dejará pasar las tramas de ambos sentidos, desde el servidor hasta los switch y viceversa, por lo que por ende se debe colocar el mismo en este segmento de red. Al realizar esta acción y colocar una máquina que posea Wireshark se podrá observar de una manera pasiva todas estas tramas que fluyen desde y hacia el servidor y con esto realizar el posterior análisis [27]. Una implementación de este tap de red se lo puede observar en la Figura 5.7. Análisis de tráfico mediante Tap de Red

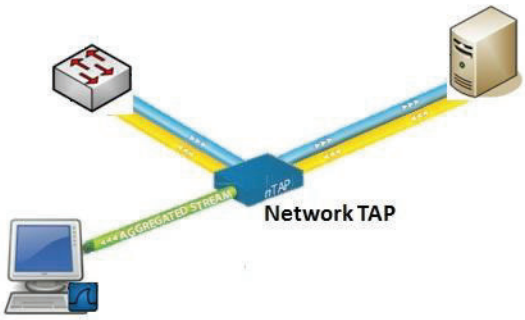


Figura 5.7. Análisis de tráfico mediante Tap de Red

5.1.1.1.6. Captura de Paquetes Remota

Se ha visto que existe la posibilidad de la captura de paquetes generalmente involucrándonos en el segmento entre el servidor y el switch, pero si se puede tener acceso al servidor de la red, se puede realizar ciertas instalaciones en el mismo, lo

cual nos garantizará poder realizar el monitoreo de tráfico desde el servidor hacia los host requerido en la red.

Para poder implementar este método de captura de paquetes, basta ejecutar rpcapd.exe, que viene incluido en el software WinPcap (Software de código abierto que básicamente permite la captura de paquetes en la red y el posterior envío de los mismos, sin necesidad de que estos pasen por la pila de protocolos, para su posterior análisis con alguna de las herramientas analizadoras de paquetes que en este caso será Wireshark) [51]. En esta herramienta se puede especificar el puerto de escucha, host a cuál se desea establecer el contacto, posibilidad de autenticar, entre otras.

Para dar inicio al servicio basta iniciar la consola de comandos y ejecutar el comando: `rpacapd.exe -n -p 8080` (teniendo en cuenta que en este caso el puerto de escucha es el 8080) [47]. Esto se puede visualizar en la Figura 5.8. Captura de datos con rpcapd

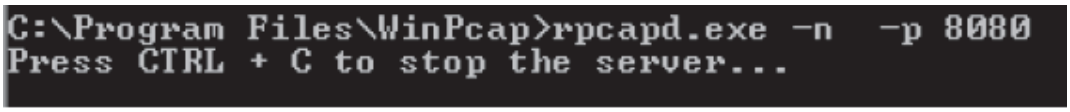


Figura 5.8. **Captura de datos con rpcapd**

En el cliente a su vez se especificará dirección, puerto, credenciales (en caso de ser requerido) e interfaz por donde se realizará la captura de paquetes. Estas acciones del cliente se las debe realizar en Wireshark desde el menú: *Capture* >> *Options* >> *Manage Interfaces* >> *Remote Interfaces* >> + (En la versión de Wireshark 2.0.1.). Esto se puede visualizar en la
Figura 5.9. Configurar cliente para captura remota en **Wireshark**

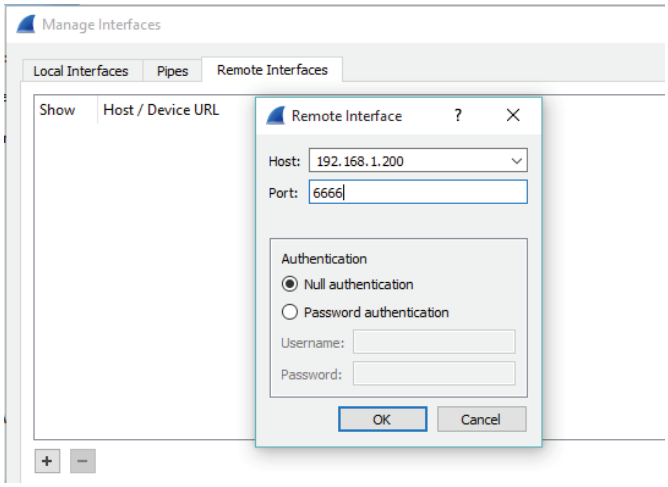


Figura 5.9. **Configurar cliente para captura remota en Wireshark**

Una configuración más específica se encuentra en el artículo “Remote Capture” que nos ofrece winpcap.org [52].

5.1.1.2. Conclusiones

Una vez definidos los requerimientos para caracterizar el sistema se concluye que en el primer formulario que se encuentran en el Anexo I se debe abarcar lo siguiente:

- Definición de dónde se realizará la evaluación del riesgo de la red específicamente (incluyendo organización, departamento, área, etc.).
- Definición clara del alcance del esfuerzo, es decir, especificar desde dónde y hasta dónde llegará la evaluación del riesgo, incluyendo los recursos e información que constituyen al sistema. Este punto es clave ya que si no se encasilla correctamente el problema, se generará una posible caracterización del sistema mayor a la requerida.
- Definir responsables de los recursos del sistema de TI, su entorno operativo y también las técnicas de recopilación de información que se pueden utilizar para solicitar la información pertinente para el entorno de ejecución del sistema de TI.
- Reconocer el entorno dónde se realizará el análisis de riesgo para lo cual se requiere conocer el funcionamiento de la red, de cómo se encuentra estructurada, y los debidos accesos que se tiene a esta. En este paso se define dónde se ubicará la herramienta para el análisis de tráfico de red, así como también cual será la técnica para realizar la captura para recopilar los datos necesarios para el análisis.

5.1.2. Identificación de la Amenaza

En este paso de la metodología el objetivo es identificar la fuente de riesgo potencial. Hay que tener cuenta que una fuente de amenaza no se considera como riesgo si no existe una vulnerabilidad que pueda ser explotada. Una fuente de amenaza puede ser cualquier circunstancia o evento con el potencial de causar daño a un sistema informático, que en este caso estará enfocado a amenazas en el tráfico de red.

Para este paso se requiere establecer una lista de fuentes de amenazas en el tráfico de red para lo cual tenemos el sniffer de red seleccionado, el cual mediante la captura de tráfico, nos facilitará la identificación de estas. Se debe tomar en cuenta que no solo se puede utilizar la herramienta de captura de tráfico para la detección de

amenazas, sino que también puede ser apoyada por alguna o algunas otras herramientas para el análisis del tráfico capturado, entre estas herramientas se consideran a: Steelcentral Packet Analyzer, Microsoft Message Analyzer, Capinfos, Nmap, Microsoft Network Monitor, entre otras [53] [54] [55]. Entonces, en este punto se requiere vincular la herramienta para realizar la captura de los paquetes y la detección de amenazas en el tráfico de red, para lo cual nos referiremos a los pasos de: “Captura” y “Análisis” de tráfico de red definidos en anteriormente.

5.1.2.1. Captura

La interfaz gráfica que nos provee Wireshark, nos presenta un proceso de captura mucho más descriptivo para el entendimiento en el proceso de captura de paquetes. Su interfaz ha ido variando en torno a la versión de la herramienta pero su interfaz principal nos presenta cinco áreas como se puede observar en la Figura 5.10. Interfaz gráfica de Wireshark [47].

Estas áreas son:

- Área 1: Controles
- Área 2: Filtros
- Área 3: Paquetes Capturados
- Área 4: Cabeceras por Capas
- Área 5: Paquete Hexadecimal

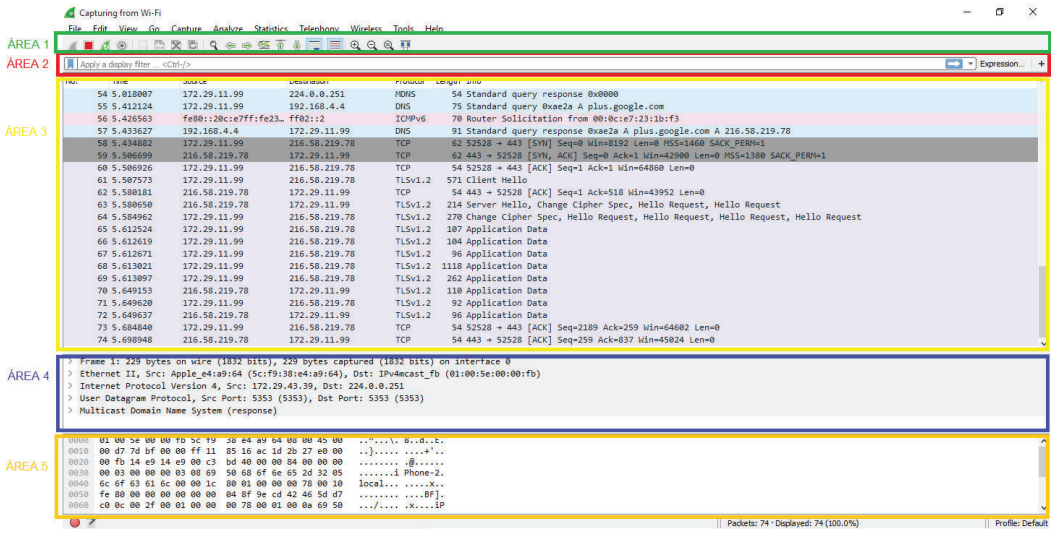


Figura 5.10. Interfaz gráfica de Wireshark

Controles: nos brinda el manejo general de la herramienta. En esta sección se encuentra los botones para empezar y detener la captura, reiniciar una captura previa, guardar o abrir un archivo de captura, buscar un paquete específico en la captura, flechas para navegar entre paquetes, la opción de mostrar los paquetes por colores dependiendo las reglas establecidas, y opciones de zoom in y zoom out.

Filtros: establece los filtros para que en la captura, sea en el archivo temporal o en alguna dirección específica, no se muestren todos los paquetes capturados sino más bien se enfoca en los paquetes que son de interés para el análisis, esto es conveniente cuando la red está ocupada o si queremos enfocarnos en un tráfico específico permitiéndonos así establecer patrones de búsqueda [27] [47].

Paquetes Capturados: muestra una lista de todos los paquetes que están siendo capturados en tiempo real, la información mostrada en esta sección corresponde al número de paquete capturado, el tiempo al que fue capturado el paquete desde el inicio de la captura, la dirección de origen y destino del paquete, el protocolo que está utilizando este paquete para su comunicación, la longitud del paquete que se está enviando, y la información de este paquete. Todos los campos obtenidos nos permiten en ocasiones determinar el problema que se tiene en la red sin necesidad muchas veces de hacer un análisis extensivo.

Cabeceras Por Capas: muestra la información por capas de cualquier paquete que se selecciona del área “Paquetes Capturados”, al desglosar los paquetes, se desglosan las cabeceras por capas, y nos permite una mayor facilidad para navegar entre los campos de las mismas.

Paquete Hexadecimal: muestra un formato hexadecimal del paquete seleccionado en el área “Paquetes Capturados”. Nos muestra una información en bruto del paquete tal y como fue capturado por la tarjeta de red, la cual se está utilizando en la captura.

5.1.2.2. Análisis

Después de realizar el proceso de captura de paquetes se llega a la parte clave en donde se debe analizar los paquetes capturados para detectar vulnerabilidades o tráfico amenazante también denominado tráfico sospechoso. Esta sección nos mostrará principalmente lo que se define como tráfico sospechoso y cómo identificar

las amenazas más comunes que pueden aparecer en una LAN, esto se logrará analizando el análisis del tráfico de red.

Al referirnos a tráfico sospechoso se hace referencia al tráfico que no concuerda con las bases de referencia de la red. Este tráfico puede estar fuera de las bases de referencia ya que el paquete podría estar usando un protocolo diferente al habitual, un puerto que no es el usual, la frecuencia con la que este paquete aparece, peticiones irregulares del paquete, respuestas, etc. El tráfico sospechoso es aquel que no es habitual en las comunicaciones y además es tráfico que no sigue patrones usuales. Este tráfico sospechoso puede darse no sólo por ataques e intromisiones en la red, sino que puede deberse también al mal comportamiento de ciertas aplicaciones, mal configuración, errores inocentes o aparatos defectuosos.

Para poder identificar tráfico sospechoso, en primer lugar se necesita identificar lo que es un tráfico común. Es aquí donde el listado de referencia de protocolos usados (comúnmente en nuestra organización) es un recurso indispensable para la persona que va a analizar la red [27, p. 382]. Si no se posee un registro de protocolos comunes en la organización, se debe analizar junto con el analista de redes de la organización el tráfico capturado, para lograr determinar si es o no un tráfico sospechoso, otra alternativa es utilizando una herramienta para análisis de tráfico capturado como las mencionadas en la Sección 5.1.2, y determinar junto al analista de redes en la organización, si son protocolos habituales o no.

5.1.2.2.1. Detectar Ataques de ARP Spoofing

Anteriormente se mencionó el ARP Spoofing como método para la captura de paquetes en la red en la Sección 5.1.1.1.4. Este método como se mencionó, se lo puede considerar agresivo ya que generalmente es utilizado como ataque a la red, consistiendo en una intromisión no autorizada en la red entre uno o varios equipos, para capturar, interceptar e incluso modificar los paquetes que llegan a esta red. Este ataque está basado en el protocolo ARP.

Básicamente lo que realiza este protocolo es encontrar la dirección MAC que corresponde a una determinada dirección IP. Para esto lo que se envía es un “ARP request”, a la dirección broadcast de la red (dirección con la que se realiza un llamado a toda la red) que contiene la dirección IP solicitada, y entonces se espera un “ARP Reply” con la dirección MAC que corresponde. Cada equipo al que se hace llamado en

la red mantiene la dirección traducida y lista en su caché para así evitar retardo en la carga. [56] Una imagen sobre el funcionamiento del mismo se puede observar en la Figura 5.11. Funcionamiento de ARP [56].

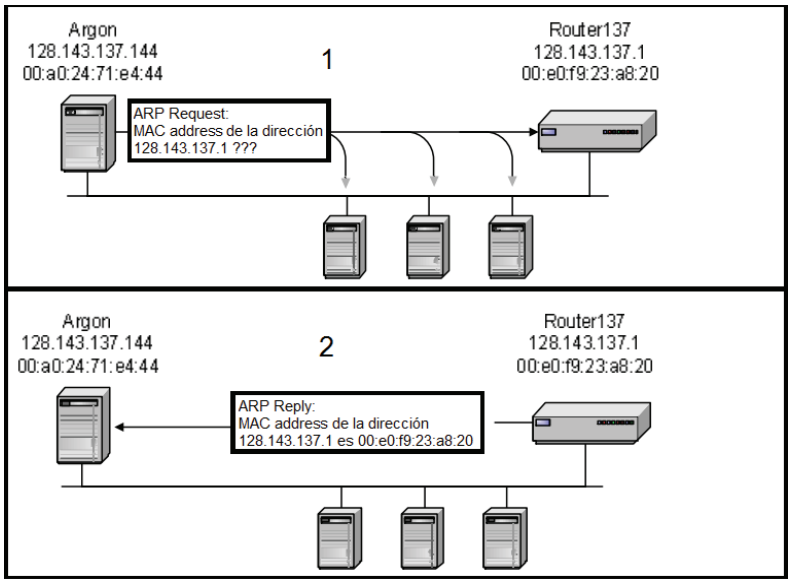


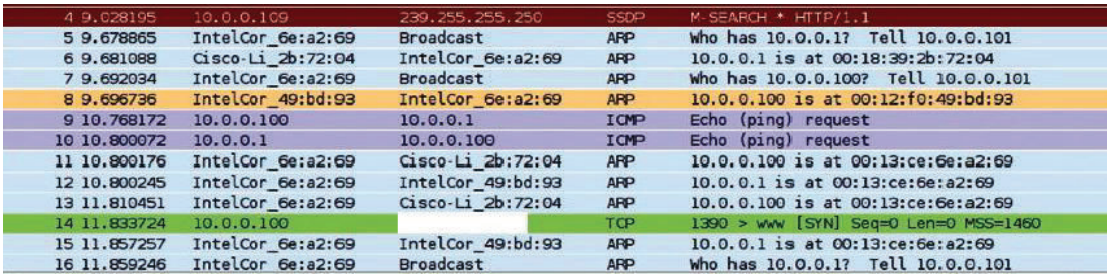
Figura 5.11. Funcionamiento de ARP

- **Identificar ARP Spoofing con Wireshark**

A continuación se evalúa el caso plateado en la Figura 5.12. Detección de Ataque por ARP Spoofing. El tráfico capturado en su quinto paquete detecta una máquina con dirección IP 10.0.0.101 y MAC IntelCor_6e:a2:69, lanzando un ARP request preguntando por la dirección MAC de la IP 10.0.0.1 es decir la compuerta de la red. Seguidamente en el paquete número 6, el router a cargo responde esta solicitud con la ARP reply correspondiente a la dirección MAC requerida. En el paquete número 7 nos muestra a esta misma máquina enviando un ARP request por la MAC que corresponde a la IP 10.0.0.100 (que en este caso corresponde al servidor de ficheros), una vez más en el paquete número 8 responde esta vez el servidor con su dirección MAC.

Hasta aquí lo que la máquina con IP 10.0.0.101 y MAC IntelCor_6e:a2:69 ha conseguido es la dirección física tanto del router como del servidor, pero he aquí donde empieza el problema ya que observando a los paquetes 11, 12 y 13, la máquina envía reiteradamente paquetes falsos ARP Reply donde asocia su propia dirección MAC con las direcciones IP tanto del router como del servidor, logrando así

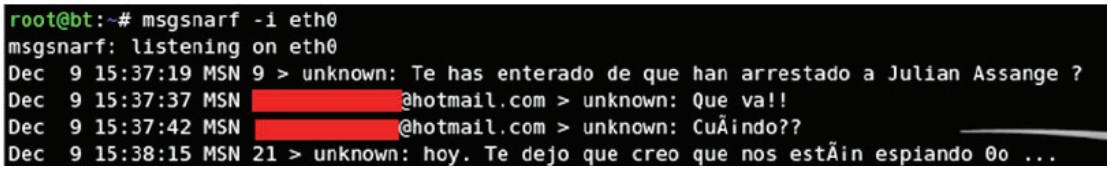
que todo el tráfico que circule entre la compuerta de la red y el servidor, pase también por la máquina que está realizando el ataque.



4	9.028195	10.0.0.109	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1
5	9.678865	IntelCor_6e:a2:69	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.101
6	9.681088	Cisco-Li_2b:72:04	IntelCor_6e:a2:69	ARP	10.0.0.1 is at 00:18:39:2b:72:04
7	9.692034	IntelCor_6e:a2:69	Broadcast	ARP	Who has 10.0.0.100? Tell 10.0.0.101
8	9.696736	IntelCor_49:bd:93	IntelCor_6e:a2:69	ARP	10.0.0.100 is at 00:12:f0:49:bd:93
9	10.768172	10.0.0.100	10.0.0.1	ICMP	Echo (ping) request
10	10.800072	10.0.0.1	10.0.0.100	ICMP	Echo (ping) request
11	10.800176	IntelCor_6e:a2:69	Cisco-Li_2b:72:04	ARP	10.0.0.100 is at 00:13:ce:6e:a2:69
12	10.800245	IntelCor_6e:a2:69	IntelCor_49:bd:93	ARP	10.0.0.1 is at 00:13:ce:6e:a2:69
13	11.810451	IntelCor_6e:a2:69	Cisco-Li_2b:72:04	ARP	10.0.0.100 is at 00:13:ce:6e:a2:69
14	11.833724	10.0.0.100	[redacted]	TCP	1390 > www [SYN] Seq=0 Len=0 MSS=1460
15	11.857257	IntelCor_6e:a2:69	IntelCor_49:bd:93	ARP	10.0.0.1 is at 00:13:ce:6e:a2:69
16	11.859246	IntelCor_6e:a2:69	Broadcast	ARP	Who has 10.0.0.1? Tell 10.0.0.101

Figura 5.12. Detección de Ataque por ARP Spoofing

Este proceso de ataque puede ser generado no solo por expertos sino que existen herramientas tales como: Ettercap, ARPwner, Cain y Abel [57] [58], entre otras relativamente fáciles en su manejo las cuales sin tener mucho conocimiento permiten realizar un ataque por lo que el riesgo de un ataque de este tipo es alto, una visualización de este ataque puede visualizarse en la Figura 5.13. Ataque Arp Spoofing con la herramienta DSniff.



```
root@bt:~# msgsnarf -i eth0
msgsnarf: listening on eth0
Dec  9 15:37:19 MSN 9 > unknown: Te has enterado de que han arrestado a Julian Assange ?
Dec  9 15:37:37 MSN [redacted]@hotmail.com > unknown: Que va!!
Dec  9 15:37:42 MSN [redacted]@hotmail.com > unknown: CuÃindo??
Dec  9 15:38:15 MSN 21 > unknown: hoy. Te dejo que creo que nos estÃin espiando 0o ...
```

Figura 5.13. Ataque Arp Spoofing con la herramienta DSniff

Para detectar este ataque basta con identificar paquetes “ARP reply” sospechosos que se envíen constantemente y analizar en qué consiste la trama de este paquete. Si lo que está realizando es forzar a que todo el tráfico que esté pasando se redirija a otro dispositivo sea este el dispositivo atacante u otro dispositivo el cuál no corresponda al switch, router, servidor o dispositivo propio que deba manejar este tráfico, pues se halla en presencia en un ataque “ARP Spoofing”.

5.1.2.2.2. Detectar Ataques MAC Flooding

- **Asignación MAC-Puerto**

Para entender lo que es un ataque MAC flooding, se debe entender primero como funciona la asignación de puertos en un switch. Cuando un equipo se conecta a la red de área local, envía una trama conteniendo la dirección MAC de esta. Cuando esta

trama llega al switch, este hace el ingreso de esta dirección MAC que venía en la trama en una memoria llamada CAM (Content-Addressable Memory), la cual realiza una entrada a la tabla donde asigna la MAC con el puerto correspondiente en donde se encuentra el equipo, así que cuando llegase un paquete dirigido a este equipo, el switch ya sabe por cual puerto debe enviarlo, y en el caso de que no esté registrado aún el puerto de dicha MAC pues lo envía a todos los puertos exceptuando por el que llego la trama, para que así el destinatario correcto reciba el paquete y al momento de responder, el switch pueda realizar la respectiva correspondencia MAC-puerto y almacenar en su memoria CAM.

- **Identificar MAC Flooding con Wireshark**

El ataque MAC flooding consiste en anular el switch, al cual se lo "inunda" con diferentes paquetes falsificados los cuales contienen diferentes direcciones MAC de origen, llegando a llenar la memoria CAM del switch y haciendo que el switch entre en un estado llamado "fallo en modo de apertura", en la que todos los paquetes que llegan al switch van a ser enviados por todos los puertos (como si se tratara de un hub), en vez de ser enviado únicamente por el puerto correcto de acuerdo al funcionamiento normal [59]. Un ataque de este tipo puede ser generado por varias herramientas, un claro ejemplo se tiene en la Figura 5.14. Mac Flooding con Macof, donde se genera un ataque con la herramienta Macof indicándole que se debe realizar un ataque a la interfaz eth0 mandándole 1000 paquetes falsificados para que así el switch llene su memoria CAM.

```
root@bt:~# macof -i eth0 -n 1000
9e:3:2b:0:d:c8 ee:b0:d9:6c:e4:8b 0.0.0.0.63518 > 0.0.0.0.55376: S 1811335234:1811335234(0) win 512
c4:9f:8d:1f:d5:31 6b:82:fd:7e:f9:de 0.0.0.0.35857 > 0.0.0.0.62832: S 1603328042:1603328042(0) win 512
bd:1f:62:4e:ae:8c ab:b8:28:56:1a:6a 0.0.0.0.62505 > 0.0.0.0.8561: S 804371142:804371142(0) win 512
a7:75:21:2f:80:ee 65:a3:a1:60:90:42 0.0.0.0.60476 > 0.0.0.0.62084: S 224272867:224272867(0) win 512
25:89:a2:73:92:ee 4a:4b:1:7:30:7e 0.0.0.0.4970 > 0.0.0.0.22943: S 1324361036:1324361036(0) win 512
66:61:3d:d:5b:62 56:94:7c:43:77:7d 0.0.0.0.35896 > 0.0.0.0.49311: S 1541919794:1541919794(0) win 512
```

Figura 5.14. Mac Flooding con Macof

Para identificar este ataque basta con observar el tráfico de este segmento con Wireshark, y se vería una gran cantidad de tramas malformadas con valores al azar como lo observado en la Figura 5.15. Ataque Mac Flooding en Wireshark.

346	13.300620	39.39.218.123	67.129.128.67	TCP	[Malformed Packet]
347	13.301344	65.30.29.120	192.164.170.9	TCP	[Malformed Packet]
348	13.302264	82.8.242.103	225.173.109.6	TCP	[Malformed Packet]
349	13.303184	88.125.244.10	81.219.96.39	TCP	[Malformed Packet]
350	13.305176	92.236.234.36	103.223.24.56	TCP	[Malformed Packet]
351	13.306176	40.255.13.13	57.31.185.74	TCP	[Malformed Packet]

Figura 5.15. Ataque Mac Flooding en Wireshark

La razón de tener “Malformed Packet” en la descripción de los paquetes, es porque la herramienta utilizada para el ataque (Macof), ensambla los paquetes sin tener en cuenta las especificaciones de encapsulamiento del protocolo. Con esto, el atacante podría colocarse dentro de la red y recibir todos los paquetes que están siendo enviados a todos los usuarios, apoderándose así de información inaccesible en un funcionamiento normal del switch.

5.1.2.2.3. Detectar Ataques de Denegación de Servicio (DoS)

Un ataque de denegación de servicio es aquel en el que el atacante intenta evitar que un usuario legítimo de la red, acceda a la información o servicios que esta provee, el atacante puede ser capaz de impedir el acceso a correo electrónico, sitios web, cuentas en línea (banca, etc.), u otros servicios a los que podría acceder el equipo afectado. Al igual que en el anterior caso, el ataque más común de denegación de servicio es cuando el atacante “inunda” la red, por ejemplo si se tiene un usuario que realiza un HTTP request (una llamada a una cierta página en internet), lo que se está realizando es una petición al servidor para poder ver la página. El servidor procesa una cierta cantidad de peticiones a la vez, pero si el atacante sobrecarga al servidor con una gran cantidad de otras peticiones, la petición original no va a poder ser procesada. [60].

- **Three Way Handshake**

Para poder analizar en mayor detalle cómo se realiza una DOS, se necesita entender cómo funciona el proceso de establecer una conexión entre un cliente y un servidor, este proceso que también recibe el nombre de negociación se la realiza en tres pasos y recibe el nombre de three way hanshake. La negociación empieza cuando el dispositivo que desee establecer la conexión envía un mensaje SYN al servidor el cual previamente tiene algún puerto a la escucha, si este no se encuentra a la escucha, el dispositivo que desee establecer la conexión recibirá un mensaje “Reset”, indicándole que la negociación no se puede realizar. Paso seguido y si el mensaje SYN fue exitoso, el servidor recibirá este SYN y responderá con el SYN que se recibió más un

mensaje ACK diciéndole al cliente que se encuentra listo para la conexión, este mensaje recibe el nombre de SYN/ACK. Finalmente el cliente recibe este mensaje SYN/ACK y retira la parte SYN del mensaje y reenvía al servidor el mensaje ACK indicándole que también se encuentra listo para la conexión completándose así este procedimiento de negociación para el establecimiento de la conexión en tres pasos [61]. Una ilustración de esta conexión se la puede visualizar en la Figura 5.16. Negociación en tres pasos (Three Way Handshake).

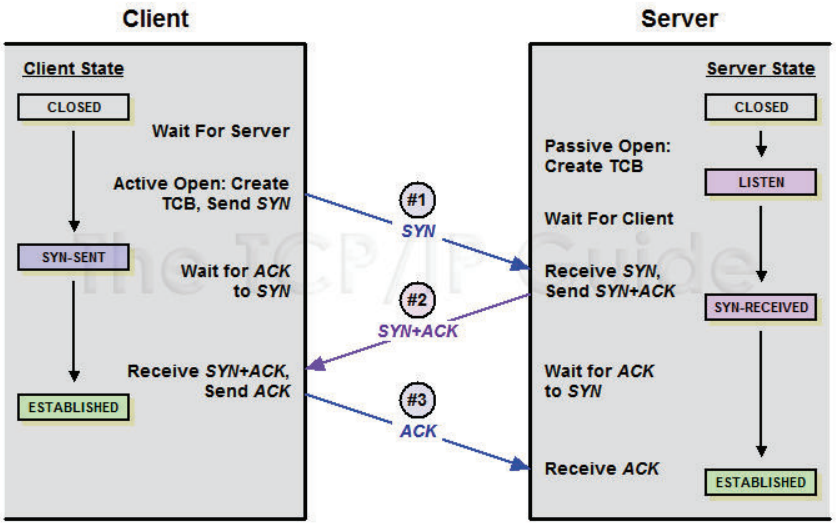


Figura 5.16. Negociación en tres pasos (Three Way Handshake)

- **Identificar DoS con Wireshark.**

Ahora si se visualiza la Figura 5.17. Ataque DOS identificado con Wireshark, se tiene un caso en el que se tiene dos máquinas, un cliente y un servidor. El cliente tiene una dirección IP 10.0.0.101 y el servidor tiene una IP 10.0.0.20 con el puerto 80 en escucha para alguna conexión, al analizar el tráfico en la herramienta Wireshark en este segmento de red, y desplegando el menú *Statistics* >> *Flow Graph,* nos indica de una forma gráfica que el cliente está enviando una gran cantidad de mensajes SYN al servidor para realizar una conexión, el servidor ha tratado de resolver la MAC de esta dirección IP algunas veces como se puede observar en el paquete 7852 de la figura, pero al no recibir la respuesta de la dirección física de la máquina, no puede enviar el ACK-SYN para continuar con la negociación en tres pasos revisada anteriormente. Esta situación conlleva a que el servidor mientras espera que le llegue la dirección física de la máquina que está tratando de establecer la conexión, siga recibiendo peticiones de conexión (mensajes SYN) que provocará que el servidor por cada

petición trate de resolver una nueva conexión. Esta estructura que identifica todas las conexiones se llama TCB (Transmission Control Block) y si se tiene una cantidad elevada de estas estructuras, se puede acabar con los recursos del servidor generando con esto que no admita más solicitudes de conexión, y así anulando al servidor para que ningún otro cliente pueda acceder a algún servicio de este [47, p. 19].

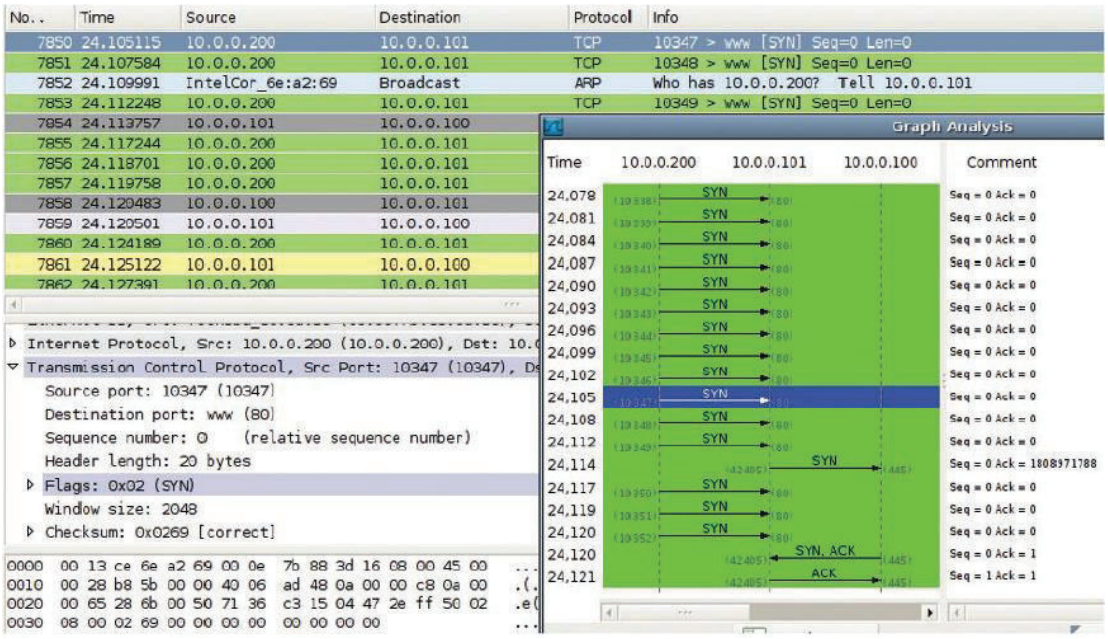


Figura 5.17. Ataque DOS identificado con Wireshark

En este caso se puede observar que identificar un ataque de DoS es relativamente simple, basta con identificar una gran cantidad de mensajes SYN para establecer una conexión en el cual el cliente envía paquetes sin esperar respuesta del servidor. Este ataque fue realizado con la herramienta hping2 aunque existen otras herramientas que permiten realizar ataques como este. Se destacan en estas a las herramientas LOIC [62] y HOIC [63] que constan con una interfaz amigable las cuales permiten realizar ataques con peticiones involucrando a los protocolos TCP o UDP e incluso HTTP, así como también la cantidad de amenazas y velocidad de envío.

5.1.2.2.4. Detectar Ataques DHCP Spoofing

Un ataque menos frecuente pero igualmente dañino es el DHCP Spoofing, el cual consiste en realizar falsificaciones de paquetes DHCP desde un servidor falso. Para

entender mejor este ataque se necesita primero tener claro el funcionamiento de un servidor DHCP y cuál es su función en la red.

- **Servidor DHCP**

Cuando un cliente se conecta a una red, este cliente necesita establecer ciertos parámetros de configuración en su tarjeta de red para que pueda pertenecer a la red en sí, entre estos parámetros se encuentra la dirección IP, la máscara de la red o subred, la compuerta, etc. Esta configuración de la tarjeta de red se la puede realizar de dos formas: una manual y una automática. La forma manual consiste en el usuario mismo de la máquina configure los parámetros de la red, para esto el usuario debería saber dentro de que red se encuentra, que IP's están disponibles en la red, cual es la dirección de la compuerta, entre otros parámetros más, pero no siempre un usuario de la red va a saber estos parámetros por lo cual, existe el servidor DHCP (la forma automática).

El servidor DHCP asigna direcciones IP, máscaras, Gateway, entre otras configuraciones a las máquinas de la red. Estas direcciones IP residen dentro de una base de datos del servidor DHCP y este sabe qué dirección asignar a cada máquina. Esta asignación es transparente para el usuario ya que cuando una máquina se conecta a la red, automáticamente se le asigna todos estos parámetros mediante el servidor DHCP. El cliente no tiene control sobre la configuración que recibe del servidor DHCP, simplemente la acepta [64].

Ahora para entender más profundamente como es que se realiza esta asignación de configuración a un dispositivo en la red, se puede identificar los siguientes pasos:

1. Al conectarse un equipo nuevo a la red, este envía una petición llamada DHCP-Discover a la dirección broadcast (dirección que llama a toda la red) esperando que algún servidor DHCP en la red le responda.
2. El servidor DHCP responde a la máquina con un paquete llamado DHCP-Offer el cual contiene los parámetros de configuración necesarios para hacerla parte de la red (IP, máscara, gateway, etc.).
3. Esta máquina que está queriendo ser parte de la red, puede ya haber recibido varios paquetes DHCP-Offer, y elige aceptar el paquete en torno al siguiente criterio: si la configuración recibida corresponde a una configuración previa que ya tuvo la máquina, pues aceptará esta configuración; pero en caso de que no haya tenido ninguna de las configuraciones recibidas, aceptará la primera oferta recibida.

4. Una vez aceptada la propuesta de configuración DHCP, la máquina enviará un paquete DHCP-Request una vez más por la dirección de broadcast pidiendo autorización para poder implementar la configuración adquirida.
5. Finalmente el servidor responderá con un paquete DHCP-ACK dirigido a la máquina si la autorización es exitosa, o a su bien un DHCP-NAK con el cual no se le autoriza para utilizar la configuración recibida [47, p. 24].

Un ejemplo claro de la negociación entre cliente y el servidor del DHCP se observa mediante el tráfico de Wireshark en la Figura 5.18. Negociación de DHCP en Wireshark.

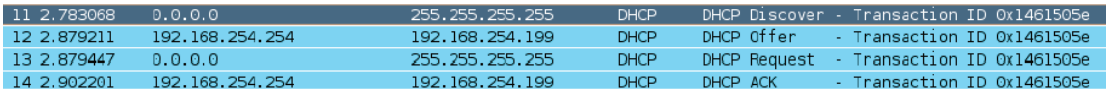


Figura 5.18. Negociación de DHCP en Wireshark

- **Identificar DHCP Spoofing con Wireshark**

Ahora bien, ya entendido el propósito del servidor DHCP y cómo es su funcionamiento, se supone un caso en el que en la red se tiene un servidor DHCP no auténtico, este servidor no necesariamente debe ser desde un dispositivo servidor sino que se puede emular un servidor DHCP en cualquier máquina. Al conectar una nueva máquina en la red, esta va a recibir varias DHCP-Offer como ya se vio en la explicación del funcionamiento del servidor DHCP, pero una de estas DHCP-Offer puede ser del servidor falso el cual le va a proporcionar información falsificada al cliente.

Un escenario común sería aquel en el que un atacante mediante el servidor DHCP falso asigne una información falsa a la máquina, indicándole que la compuerta de comunicación de la red sea la dirección propia del atacante, es decir, todo el tráfico que envíe el host va a ser enviado por la máquina atacante, y para que esta acción sea transparente al usuario, el atacante podría enrutar todos los paquetes a su destino legítimo con lo que el host con la configuración falsificada, no repare en que su información este siendo intervenida. Incluso el atacante podría brindar configuración falsa de DNS (Sistema de nombre de dominio), para así poder manipular cualquier resolución de nombres que se le presente más adelante.

Existen herramientas tales como Ettercap o Yersinia que nos permiten realizar levantamiento de servidores DHCP falsos, o incluso como se detalló anteriormente,

configurando un servidor DHCP con dhcpd3 en el equipo atacante, nos permitiría hacer una intromisión en la red mediante DHCP como la antes mencionada [47, p. 24]. Síntomas de que la red está siendo atacada, son por ejemplo duplicación de IP's o comportamiento anormal del protocolo DHCP. Un claro ejemplo de este ataque y cómo identificarlo mediante el tráfico capturado con Wireshark se puede observar a continuación. Se supone que el atacante tiene realizada la configuración de la Figura 5.19. Servidor Falso DHCP con dhcpd3 [47]. Este es un servidor falso DHCP que fue configurado mediante dhcpd3 (herramienta para levantar servidores DHCP) en algún sistema operativo Linux.

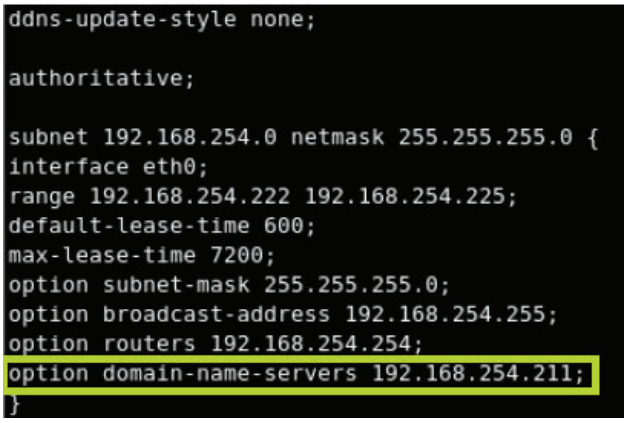


Figura 5.19. Servidor Falso DHCP con dhcpd3

En esta configuración se puede encontrar en la sección "range" un rango de cuatro direcciones IP que no se encuentran en uso, además en la dirección broadcast se encuentra la dirección del Gateway auténtico de la red, pero al momento de establecer la dirección del servidor de dominios (DNS) se establece la dirección IP del atacante de la red (192.168.254.211), para que así cuando un usuario se conecte a la red y solicite una dirección IP, el servidor falsificado dhcp le brindará toda la configuración válida, exceptuando en que la dirección del DNS estará la dirección del atacante. El atacante configura también la herramienta Ettercap [65] con el fin de falsificar respuestas DNS.

En la Figura 5.20. Fichero de Cliente con configuración DHCP falsa [47]. Se puede observar al fichero de la víctima al cual se le dio una configuración no válida del dhcp con este servidor falso, como se puede observar la configuración que se le asigna es una configuración valida exceptuando el servidor dns donde está configurada la IP del atacante.

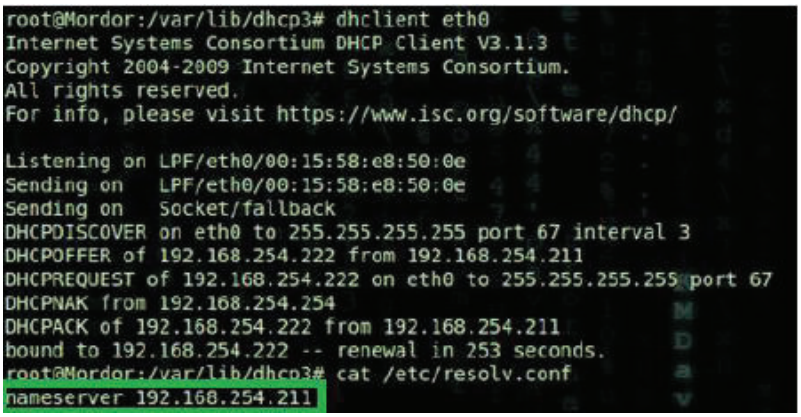


Figura 5.20. Fichero de Cliente con configuración DHCP falsa

Por otra parte en la Figura 5.21. Análisis con Wireshark, configuración DHCP no válida, se encuentra la captura de tráfico realizada con Wireshark, en esta se puede observar desde el DHCP-Request realizado por el cliente, se puede observar la DHCP-offer realizado por el servidor falso y la configuración que le brinda a la máquina atacada, aquí también se puede observar la dirección falsa del servidor de dominios que le brinda el servidor DHCP falso.

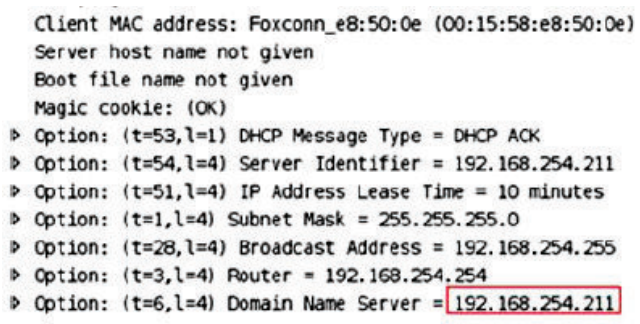


Figura 5.21. Análisis con Wireshark, configuración DHCP no válida

Si se estuviese realizando un monitoreo de la red en cuestión y se poseyera las configuraciones válidas de las mismas, se podría realizar la captura con el Wireshark y posteriormente realizar el análisis para poder observar cómo se están asignando las direcciones IP a los clientes de la red, si se destacara una asignación errónea como la observada en el ejemplo, se podría evidenciar que la red se encuentra bajo un ataque.

5.1.2.2.5. Detectar Ataques VLAN Hopping

Una red de área local generalmente en una entidad comercial, no brinda el mismo tipo de acceso a todos los usuarios de la red, una red local comercial incluye varios departamentos y pisos que puede poseer la empresa y es necesario separar estas redes en otras de acuerdo a las necesidades de cada comercio. Estas redes individuales no necesariamente deben incluir su propia infraestructura sino que pueden compartirla con los mismos dispositivos medios de todas las redes, pero aun así mantenerlas separadas del resto. Este concepto de redes locales diferentes que comparten infraestructura son también llamadas VLAN las cuales también son objeto de ataques. Así que para poder entender del ataque a estas VLAN mediante VLAN Hopping, se necesita entender primero el concepto claro de lo que es una VLAN y cómo funciona.

- **VLAN**

Una VLAN consiste en el agrupamiento lógico de estaciones finales (equipos) las cuales comparten requisitos en común, este agrupamiento es de tipo lógico ya que una VLAN no depende de la ubicación física de los equipos, es decir, una VLAN tiene los mismos atributos que una LAN física, con la diferencia que permite agrupar estaciones finales incluso si estas no se encuentran físicamente en el mismo segmento de LAN.

Las VLAN son asociadas generalmente con las subredes IP ya que, todas las estaciones finales en una subred IP en particular, pertenecen a la misma VLAN. Este tráfico entre las VLAN debe ser enrutado y esto se lo logra mediante la configuración generalmente de los switches de la red, estos dispositivos son configurados de tal manera que a cada puerto del switch se le asigna la red virtual (VLAN), es decir, si un dispositivo se conecta a este puerto, este empieza a formar parte de dicha VLAN.

Existe también otra forma para la configuración de las VLAN que es realizado mediante software, aquí se establece no solo las redes virtuales existentes sino que también se puede especificar a que VLAN corresponde cada equipo, que direcciones MAC son permitidas en la VLAN, e incluso asignación automática de VLAN indistintamente del puerto en el que se lo conecte. Estas posibles configuraciones dependerán del equipo que se esté utilizando para realizar las conexiones ya que no todos soportan las mismas configuraciones ni poseen las mismas características. Para poder saber la forma de configuración de las VLAN en cada switch basta consultar el modelo del dispositivo y el cómo se configuran las VLAN en este. Por ejemplo si se

tiene la red de la Figura 5.22. Funcionamiento de una VLAN, en la que se tiene 3 departamentos: uno de ingeniería, otro de marketing y otro de finanzas. Capa departamento con equipos en diferentes plantas de un edificio, y teniendo la necesidad de tener conexión de red en cada departamento, se realizan redes VLANs que involucren estos equipos.

Siguiendo el ejemplo de la Figura 5.22. Funcionamiento de una VLAN, se analiza el caso en que un miembro de la VLAN 10 en el piso 1 envía una trama para un miembro de la VLAN 10 en el piso 2. El Switch 1 en primer lugar identifica la VLAN por la cual se está enviando la trama sea por el puerto de conexión (puerto 1) o por el software con el que este configurado el switch, e identifica que la trama saliente pertenece a la VLAN 10, esta trama tiene también la dirección MAC de destino pero el Switch 1 no lo identifica dentro de su tabla MAC/IP de red, por lo tanto, envía la trama a todos los demás puertos que pertenecen a la VLAN 10, es decir, el puerto 4 de los switch 2 y 3. Del mismo modo, el switch 2 y 3 inspeccionan el encabezado de la trama con el fin de obtener la dirección MAC de destino. El Switch 3 no identifica esta dirección MAC en el o los puertos que pertenecen a la VLAN 10, en este caso por el puerto 1, pero el Switch 2 si identifica esta dirección MAC en los puertos que pertenecen a esta VLAN 10 que en este caso igualmente es el puerto 1, finalmente entrega la trama al destinatario correcto dentro de esta propia red virtual [66].

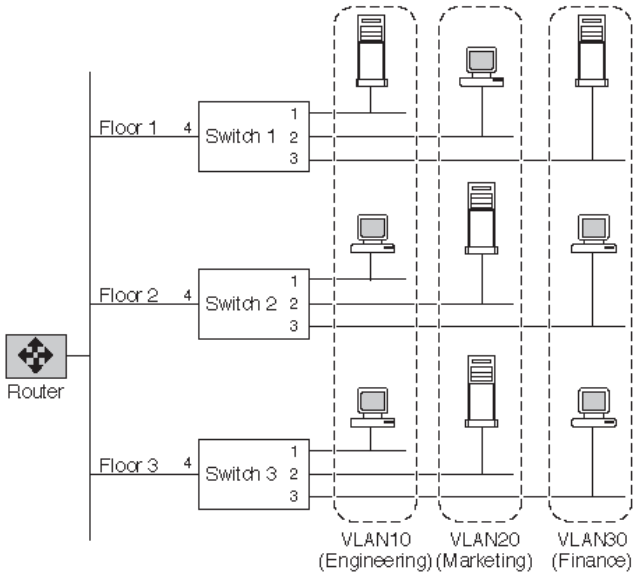


Figura 5.22. Funcionamiento de una VLAN

- **Entender el VLAN Hopping**

Teniendo ya claro el panorama de qué es una VLAN y cómo funciona, se puede entender este tipo de ataque el cual consiste en acceder al tráfico que manejan otras VLAN, diferente a la VLAN en la cual se encuentra el atacante. Este tráfico no asequible que se encuentra en otra VLAN, se lo puede acceder mediante un ataque denominado VLAN Hopping el cuál se lo realiza de dos diferentes maneras: mediante suplantación de switch y con doble etiquetado de paquetes.

- **VLAN Hopping con Suplantación de Switch**

El objetivo de la máquina atacante es acceder al tráfico de una VLAN. Esto se logra haciendo creer a los demás switches de la red que el equipo atacante es otro switch más por el cuál debe pasar todo el tráfico de red. Obviamente para lograr esto, el equipo atacante debe estar configurado de tal manera que pueda manejar los protocolos de etiquetado de paquetes (802.1Q/ISL) y concentración de enlaces (DTP) pudiendo así simular ser un switch y accediendo a todas las VLAN de la red. Además en este switch falso, los puertos deben estar configurados de forma “dynamic auto” o a su vez “desirable” lo cual se explica a continuación.

En el caso de que el switch falso se encuentre configurado de forma “dynamic auto” quiere decir que el o los puertos estarían a la escucha por tramas DTP (tramas que permiten truncar interfaces entre switches) [67]. Estas tramas son enviadas por switches vecinos. En el caso de que el switch se encuentre configurador de forma “desirable” quiere decir que el switch falso (máquina del atacante), buscará establecer enlaces con los switches vecinos mediante el envío de tramas DTP, estas tramas negociarán una conexión entre un switch auténtico de la red y la máquina atacante que esta “fingiendo” ser un switch con lo que logrará que todo el tráfico pase a través de esta [47, p. 28].

Este tipo de ataques son realizados mediante herramientas como Yersinia [68], la cual incorpora un módulo que permite el envío de paquetes DTP desde el equipo atacante hasta un switch auténtico de la red.

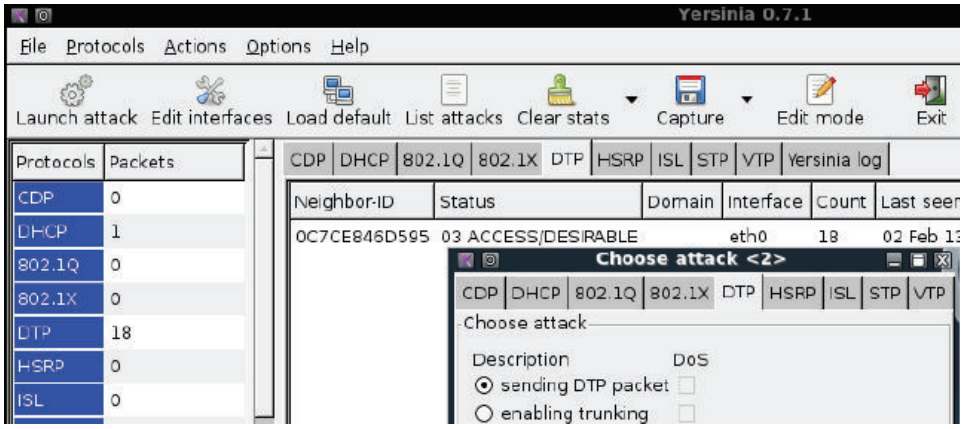


Figura 5.23. Yersinia enviando paquetes falsos DTP

Como se puede observar en la Figura 5.23. Yersinia enviando paquetes falsos DTP, los paquetes DTP son enviados al switch vecino y auténtico con dirección MAC especificada en el "Neighbor-ID". Obviamente para establecer la conexión a este switch, debe encontrarse a la escucha de paquetes DTP. Para la detección de este tipo de ataque con Wireshark, se necesita realizar la captura del tráfico de red y detectar todo tipo de paquetes DTP que están siendo enviados. Si la topología de red no ha aumentado ningún switch nuevo y se detecta paquetes DTP, se puede identificar un escenario de ataque de VLAN hopping con suplantación de switch.

Para el ataque de la Figura 5.23. Yersinia enviando paquetes falsos DTP, se tiene la captura de tráfico realizado en Wireshark en la Figura 5.24. Detección de paquetes DTP con Wireshark, en esta se puede observar los paquetes DTP que está recibiendo el switch, además se observa que para mayor facilidad de detección, en la parte de filtros se escribe DTP para que solo nos muestre el tráfico relacionado a este tipo de paquetes.

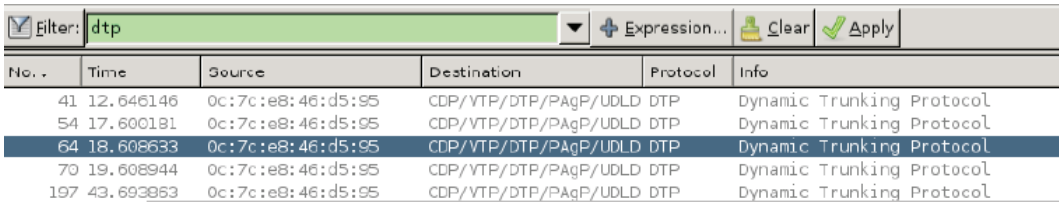


Figura 5.24. Detección de paquetes DTP con Wireshark

- **VLAN Hopping con Etiquetado Doble.**

En el funcionamiento de la pila TCP/IP cuando un usuario manda los datos desde un equipo a otro, estos datos pasan por un proceso de encapsulamiento mientras pasan

por las capas del modelo TCP/IP. De la misma forma cuando estos datos pertenecen a una VLAN, se les añade un encabezado que indica a que VLAN pertenece cada paquete y el switch es el encargado de quitar este encabezado y mandarlo por la VLAN correspondiente [47, p. 29].

En este tipo de ataque, el atacante añade un encabezado de VLAN falso, con lo cual causaría que si un atacante enviase un paquete modificado, el primer switch al que alcance el paquete identificará la VLAN del atacante sin ninguna novedad hasta este punto, pero al llegar al siguiente switch, este se encontrará con otro encabezado lo que generaría que una vez más se cambiara la ruta del paquete, enviándolo por una VLAN en principio inaccesible. Para entenderlo mejor se tiene el ejemplo de la Figura 5.25. Ataque VLAN Hopping con Doble Etiquetado.

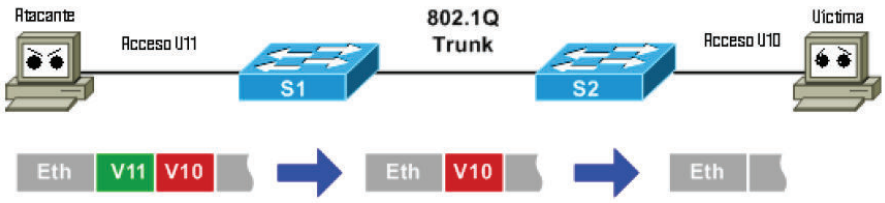


Figura 5.25. Ataque VLAN Hopping con Doble Etiquetado

En la figura se observa a un atacante que se encuentra en la VLAN 11, este envía un paquete por su VLAN añadiendo también un encabezado falso para poder acceder a la VLAN 10. El paquete alcanza al switch número 1 el cual se encarga de desempaquetar el encabezado que identifica a la VLAN del atacante que es la VLAN 11. Este mismo paquete sigue “supuestamente” sin más encabezados de VLAN hasta el siguiente switch pero en la realidad está viajando con un encabezado falso, esto causa que al momento de llegar al switch número 2, en lugar de mandarlo por la VLAN por la cual viaja que es la 11, lo vuelva a enrutar ahora por la VLAN 10 ya que eso señala su encabezado falso, Con esto se logra así que el paquete se cambie de VLAN. Este paquete ahora ya estando en una VLAN desde la cual no fue enviado, y alcanza a su víctima pudiendo así mandarle paquetes falsos que podrían generarían daño en el equipo atacado.

Con Wireshark se identifica este tipo de paquetes que contiene un doble encabezado, situándonos en el paquete y analizando su estructura. Como se puede ver en la Figura 5.26. Detección de Doble Encabezado con Wireshark [48, p. 29]. Se visualiza el paquete capturado con Wireshark con dos tipos de encabezados de identificación

VLAN, el primer encabezado que en este caso fue puesto al último por el switch, nos muestra la VLAN 11 que es la VLAN del atacante, pero en su interior se puede observar la VLAN 10 que fue puesta por el atacante al momento de mandar los datos; con esto se logra que el atacante estando en la VLAN 11 logre alcanzar la VLAN 10 al momento que el paquete llegue a otro switch.

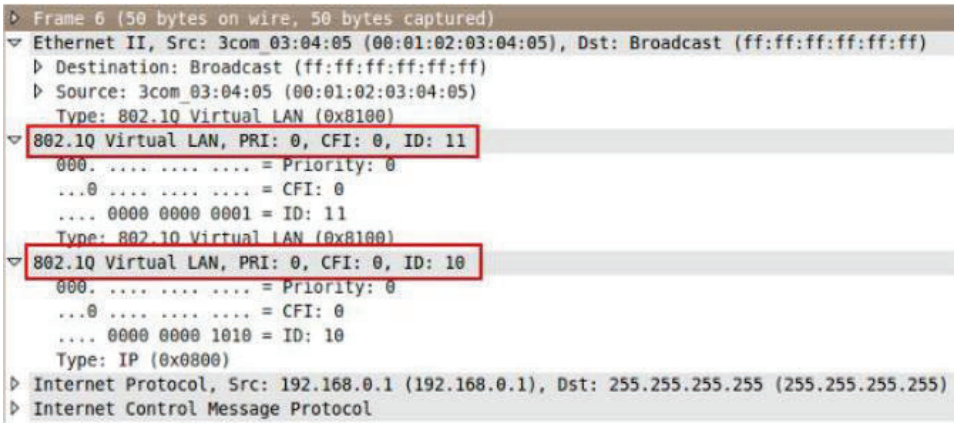


Figura 5.26. Detección de Doble Encabezado con Wireshark

5.1.2.2.6. Detectar Malware

- **Entender al Malware**

El malware, también conocido como software malicioso, es usado por cibercriminales, piratas informáticos e incluso países para irrumpir en las operaciones de un equipo o computador, robar datos personales o profesionales, cambiar controles de acceso, y en general realizar acciones nocivas para el o los host que están siendo atacados. Este software malicioso se presenta de una forma de código ejecutable, scripts, contenido activo u otra variante de software.

Actualmente, el malware se mantiene como una amenaza consistente y peligrosa, lo cual ha generado una serie de tecnologías mejoradas para la detección y prevención de este tipo de amenazas, Sin embargo, a medida que crece la tecnología de detección, los atacantes siguen evolucionando sus herramientas con el fin de mantenerse por delante de los proveedores de seguridad cada día con nuevos métodos de ataque que evadan las seguridades existentes [69, p. 3].

Nombrar todos los malware existentes hasta la actualidad es una tarea prácticamente imposible por la enorme cantidad existente y en crecimiento. En la Figura 5.27. Cantidad de malware, spam y bots por año [70], proporcionada por el reporte anual de seguridad de la “Corporación Symantec” (líder mundial como plataforma de protección de puntos finales), se puede observar las cifras críticas en torno a la seguridad informática.

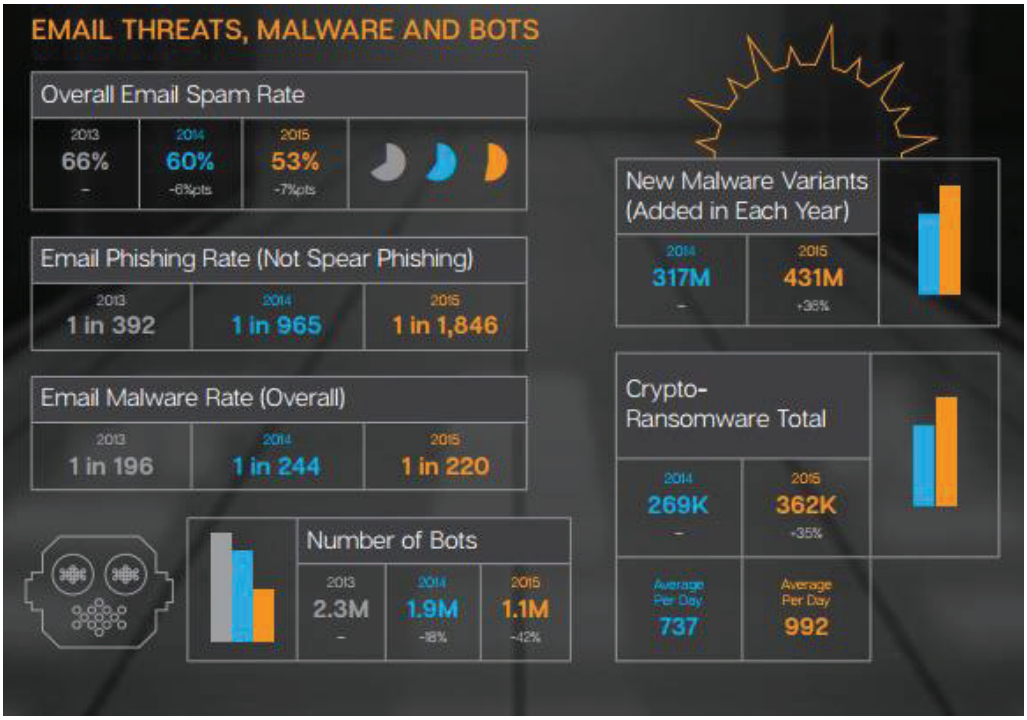


Figura 5.27. Cantidad de malware, spam y bots por año

Igualmente, haciendo referencia al artículo publicado por la CNNTech, donde la ya mencionada Symantec y Verizon (dos de las empresas más reconocidas a nivel mundial encargadas de la seguridad informática), proveen un cuadro alarmante acerca de la seguridad en la navegación en internet. Solo en el año 2015, más de 431 millones de nuevas piezas de malware fueron creadas, lo que nos dice que en promedio cerca de 1 millón de malware son creados cada día dispuestos a realizar alguna acción nociva en su ataque [71]. Por todo esto, el accionar que se debe tomar en el caso de que un equipo se encuentre infectado debe ser con la mayor rapidez, con el fin de poder minimizar el impacto, ya que no solo puede afectar al equipo atacado, sino que puede afectar prácticamente a una organización completa.

- **Caso práctico 1 de detección de malware con Wireshark**

Se tiene un equipo el cual ya se tiene conocimiento previo de que se encuentra infectado por algún tipo de malware, mas no se sabe el accionar que se debe tomar. Este equipo tenía corriendo Wireshark, capturando el tráfico diario que pasaba por él, por lo cual se decide analizar dicho tráfico. Se decide entonces aislar las IP que se encuentran implicadas en el proceso de contagio y se procede a descubrir el software descargado. Esto se logra gracias a la opción de exportar objetos de Wireshark, a la cual se accede mediante el menú *File >> Export Objects >> HTTP,* como se observa en la Figura 5.28. Exportar objetos en Wireshark.

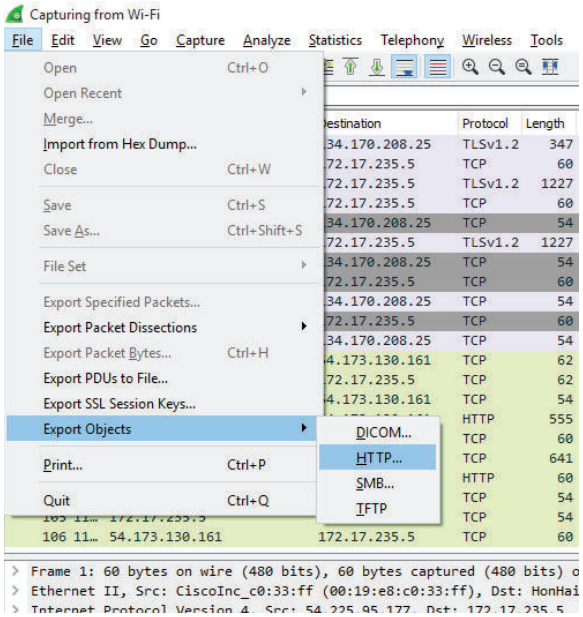


Figura 5.28. Exportar objetos en Wireshark

A continuación se despliega una nueva ventana donde se indica todas las peticiones HTTP realizadas durante toda la captura del tráfico, cada una de estas con el nombre del objeto que fue descargado, el tamaño y el lugar de donde fue descargado. Analizando el tráfico de red, se puede identificar archivos descargados de fuentes desconocidas observando el hostname que interviene en la descarga, si la dirección es ajena a las manejadas por dicho host, se debe prestar atención. En este caso práctico se puede observar que en el paquete 46 se descargó un archivo llamado “fcexploit.pdf” de un tamaño de "25169 bytes y fue descargado de la dirección “blog.honeynet.org.my”. Todo esto se puede visualizar en la Figura 5.29. Objetos HTTP capturados [47, p. 31].

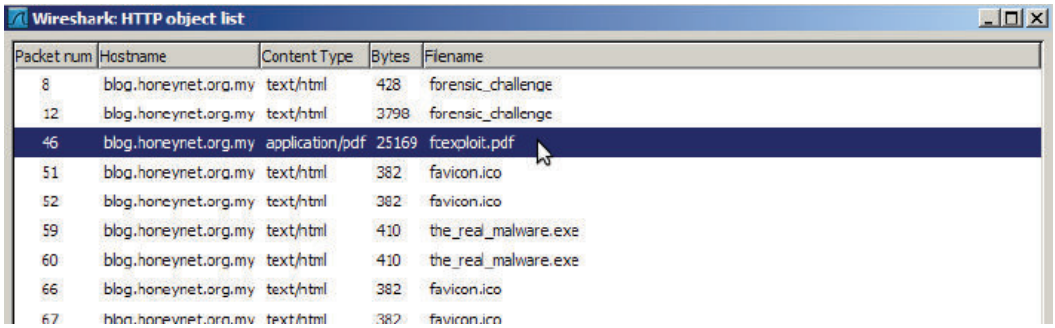
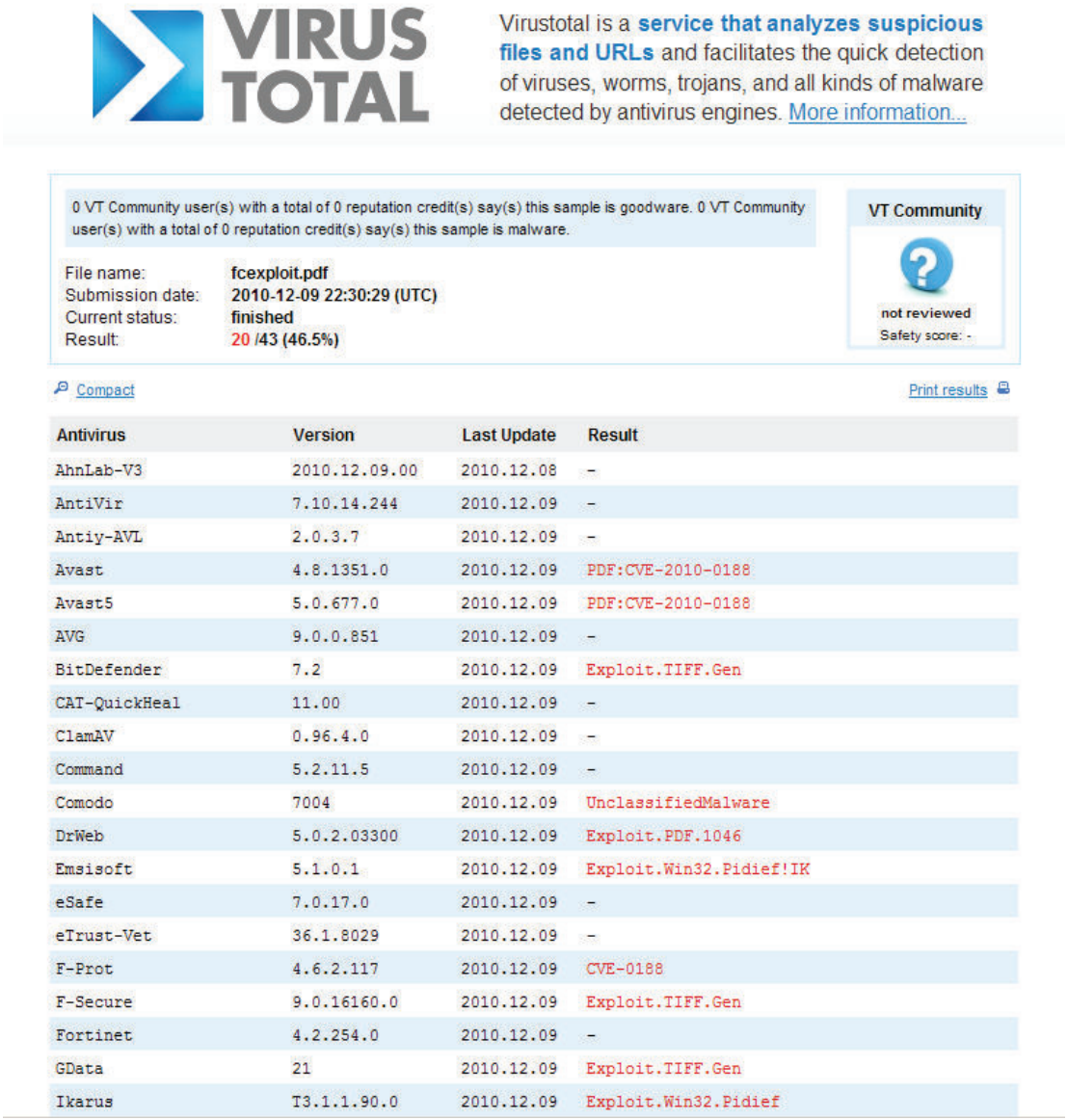


Figura 5.29. Objetos HTTP capturados

Basta con identificar el archivo que se quiere descargar para analizarlo y pulsar el botón “Save”, o en el caso de que se desee descargar todo se presiona el botón “Save All” y se almacenaría dicho archivo de forma local en el equipo. Como se tiene una lista de archivos sospechosos, se necesitaría analizar estos archivos en línea, o mediante algún antivirus, con el fin de descubrir si alguno fue el que corrompió el equipo. Hay que tener la precaución de no ejecutar los archivos sospechosos porque se puede causar un daño mayor al equipo.

En este ejemplo se analiza el archivo descargado “fcexploit.pdf” para observar si es un archivo válido, o tal vez si es alguna especie de malware. Existen páginas que permiten el análisis de estos archivos de una forma fácil con el fin de identificar si son maliciosos. Entre estas páginas se encuentra AVG Online Scanner, Dr. Web, Mxtoolbox, Virus Total, entre otros. Al hacer el análisis con la página de Virus Total (https://www.virustotal.com/), nos da el reporte completo que se puede observar en la Figura 5.30. Reporte de la página Virus Total para el análisis del archivo “fceexploit.pdf”, en la cual nos dice que efectivamente se trata de un virus. Con esto fácilmente se puede realizar la búsqueda en la web para dicho virus específico y cómo hacer para deshacernos de él [47, p. 31].



Antivirus	Version	Last Update	Result
AhnLab-V3	2010.12.09.00	2010.12.08	-
AntiVir	7.10.14.244	2010.12.09	-
Antiy-AVL	2.0.3.7	2010.12.09	-
Avast	4.8.1351.0	2010.12.09	PDF:CVE-2010-0188
Avast5	5.0.677.0	2010.12.09	PDF:CVE-2010-0188
AVG	9.0.0.851	2010.12.09	-
BitDefender	7.2	2010.12.09	Exploit.TIFF.Gen
CAT-QuickHeal	11.00	2010.12.09	-
ClamAV	0.96.4.0	2010.12.09	-
Command	5.2.11.5	2010.12.09	-
Comodo	7004	2010.12.09	UnclassifiedMalware
DrWeb	5.0.2.03300	2010.12.09	Exploit.PDF.1046
Emsisoft	5.1.0.1	2010.12.09	Exploit.Win32.Pidief!IK
eSafe	7.0.17.0	2010.12.09	-
eTrust-Vet	36.1.8029	2010.12.09	-
F-Prot	4.6.2.117	2010.12.09	CVE-0188
F-Secure	9.0.16160.0	2010.12.09	Exploit.TIFF.Gen
Fortinet	4.2.254.0	2010.12.09	-
GData	21	2010.12.09	Exploit.TIFF.Gen
Ikarus	T3.1.1.90.0	2010.12.09	Exploit.Win32.Pidief

Figura 5.30. Reporte de la página Virus Total para el análisis del archivo "fceexploit.pdf"

- **Caso práctico 2 de detección de malware con Wireshark**

El siguiente caso analiza la detección de un bot malicioso que ha infectado un host. En primer lugar el usuario detecta un comportamiento extraño en su equipo por lo cual decide realizar la captura del tráfico, Figura 5.31. Host Infectado, captura de tráfico con Wireshark La captura es realizada desde el momento en que la interfaz de conexión se pone en funcionamiento [27].

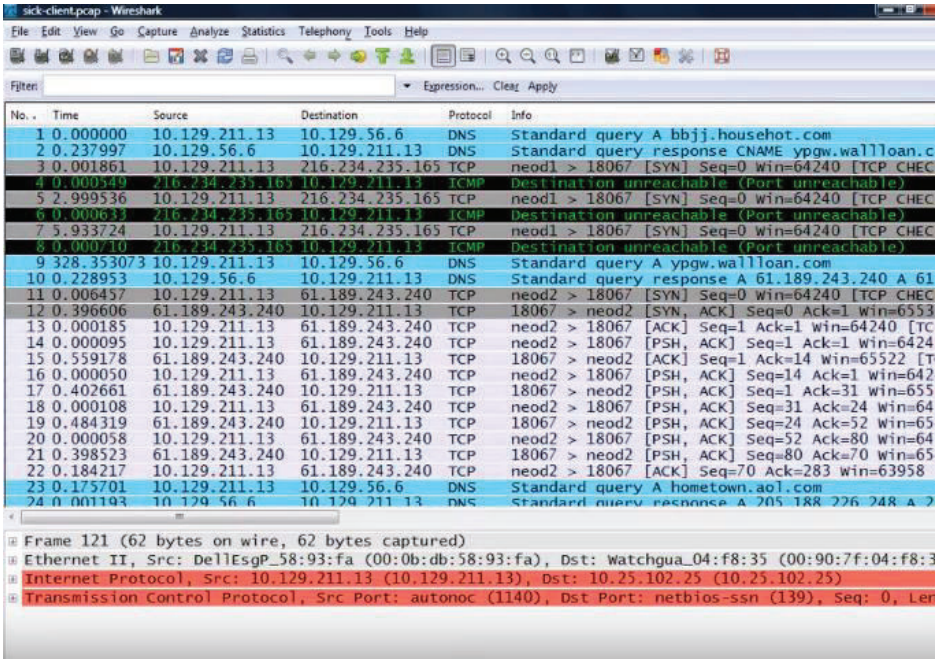


Figura 5.31. Host Infectado, captura de tráfico con Wireshark

En el tráfico de la Figura 5.31. Host Infectado, captura de tráfico con Wireshark, se observa en el primer paquete al host infectado con la dirección 10.129.211.13, el cuál realiza una consulta DNS para resolver la dirección “bbjj.household.com”. En este punto se podría realizar el proceso de el caso de estudio anterior y buscar mediante el browser esta dirección (lo cual se realizará posteriormente), y se encontrará información del atacante de una manera sencilla. Pero en el caso de que se necesite más información de cómo está funcionando este atacante, se sigue con el proceso de análisis.

En el segundo paquete, se puede observar al servidor DNS respondiendo a la solicitud con el nombre canónico (nombre auténtico) de la dirección “bbjj.household.com” la cual es “ypgw.wallloan.com”. Además en la Figura 5.32. Respuesta de DNS de página sospechosa, analizando la respuesta DNS recibida en el paquete 2, se observa todas

las direcciones IP asociadas con ese nombre de dominio en la sección “Answers RRs”. En este punto nos llama la atención ya que las respuestas de dirección obtenidas son 12 y en una conexión regular DNS las respuestas generalmente varían entre 1 a 5 direcciones según Laura Chappell directora de Wireshark University y autora del libro “Wireshark Network Analysis” [27].

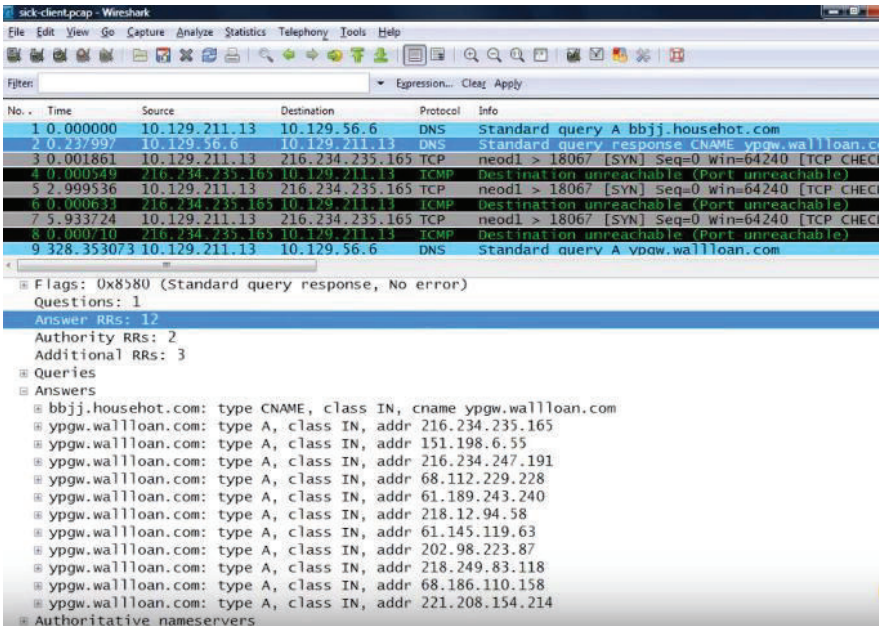


Figura 5.32. Respuesta de DNS de página sospechosa

Posteriormente ya teniendo las direcciones IP de la página solicitada, el host trata de establecer conexión con esta página por el puerto 18067 (puerto totalmente desconocido y no utilizando en la red). Pero a primera vista en los paquetes del 3 al 8 se puede evidenciar el intento de “hand-shake” a la primera dirección dada por el servidor DNS (216.234.235.165), pero como se puede observar no se logra satisfactoriamente. Lo intenta dos veces más y el host se da por vencido ya que la dirección con la cuál se trata de realizar conexión no es alcanzada.

En la Figura 5.33. Segunda respuesta de DNS a página sospechosa, en el paquete 9, una vez más el host infectado realiza el mismo proceso anterior pidiendo resolución de nombre a la misma dirección pero ya con el nombre auténtico “ypgw.wallloan.com”, y en el 10 recibe la respuesta de DNS una vez más con un número igualmente elevado de direcciones asociadas con esta página (11 direcciones), las cuales son diferentes a la primera respuesta DNS. Una vez más, esto marca una alerta ya que el servidor DNS está respondiendo con un número elevado de direcciones.

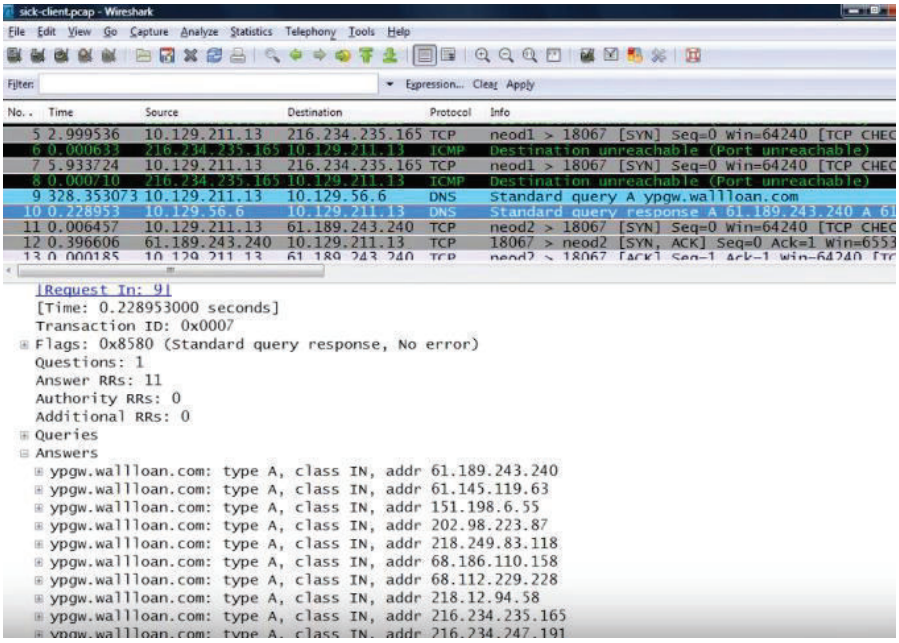


Figura 5.33. Segunda respuesta de DNS a página sospechosa

Pero en esta ocasión, al momento de que el host infectado con dirección 10.129.211.12 trata de establecer el "hand-shake" a la dirección provista por él servidor, lo logra. Esto se puede observar en los paquetes 11, 12 y 13 de la Figura 5.34. Three Way Hand Shake entre host infectado y página sospechosa

Además en el misma captura de tráfico como se evidencia en la Figura 5.34. Three Way Hand Shake entre host infectado y página sospechosa, podemos observar que el host infectado empieza a mandar información al servidor al cuál estableció la conexión utilizando paquetes "PSH, ACK" (paquetes no comunes en una red), esto se puede observar desde el paquete número 14 en adelante. Estos paquetes PSH ACK son utilizados para forzar el enviado inmediato de los datos tan pronto como sea posible y para que el TCP/IP receptor entregue los datos inmediatamente a la aplicación destino sin ponerlos en un buffer o esperar a más datos [72].

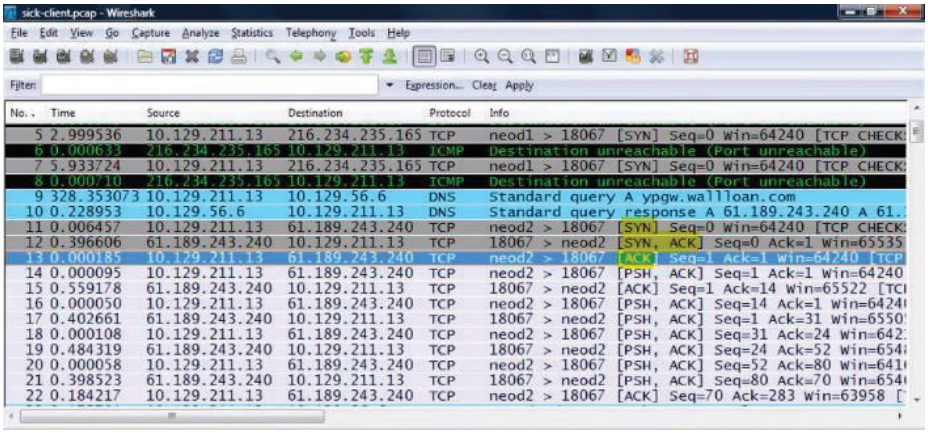


Figura 5.34. Three Way Hand Shake entre host infectado y página sospechosa

Ahora bien, recapitulando hasta este punto se tiene el host infectado que establece conexión por el puerto 18067 (puerto desconocido en la red) con la página bbjj.household.com, que en realidad tiene un nombre de dominio auténtico ypgw.wallloan.com. El servidor DNS de la página nos está devolviendo una cantidad de direcciones mayor a lo común por lo que se considera una página sospechosa. Una vez que el host establece conexión con la página indicada, empieza a enviar cierta información a la página sospechosa con la cual se hizo conexión.

En este punto el interés puede centrarse en saber qué es lo que se está enviando a la página destino, por lo cual la manera más simple es haciendo clic derecho sobre cualquiera de los paquetes PSH, ACK que está enviando el host a la página sospechosa, y a continuación dar clic en “Follow TCP Stream” (Ya que son paquetes TCP), este proceso se puede visualizar en la Figura 5.35. Siguiendo Trama TCP.

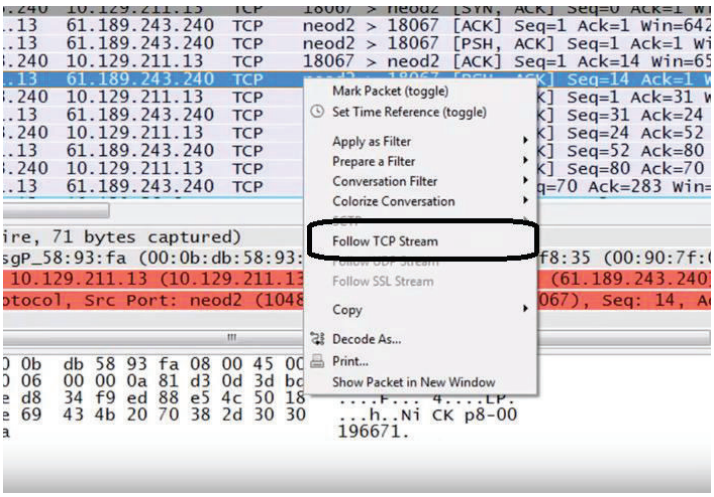


Figura 5.35. Siguiendo Trama TCP

A continuación en la Figura 5.36. Comunicación entre host y atacante, se observa en la ventana que se nos despliega, la comunicación que está manteniendo el host con la página destino. Por los comandos utilizados (user, nick, join) se puede reconocer que se trata de una comunicación IRC (Internet Relay Chat - protocolo para comunicación parecido al chat que no requiere una conexión previa entre los usuarios y es orientado a grandes grupos de usuarios en lugar de conexiones uno a uno [30]. Esta comunicación nos indica en color rojo los datos enviados desde el cliente hacia la página destino, y en color azul la respuesta hacia el host infectado.

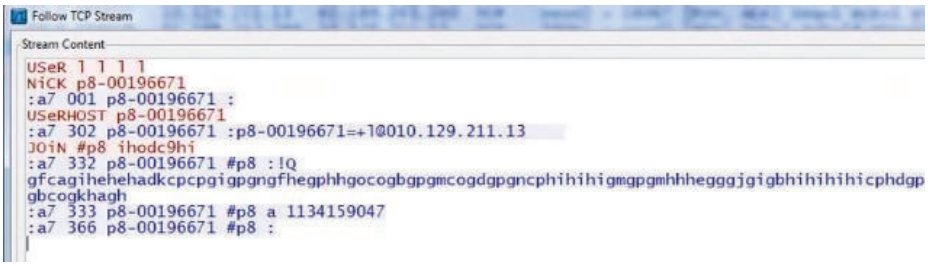


Figura 5.36. Comunicación entre host y atacante

Ahora bien, estos datos que se están enviando entre el host y la página atacante, puede que no nos den una visión clara de lo que está sucediendo, por lo cual vale la pena seguir analizando el tráfico que le sigue a la comunicación que se está manteniendo.

Este tráfico capturado en la Figura 5.37. Escaneo de puertos por bot malicioso, nos indica a host con dirección 10.129.211.3 enviando paquetes TCP hacia una gran cantidad de dispositivos en la columna de “destination” tratando de encontrar otros dispositivos en la red para poder realizar una conexión con ellos también, esto se deduce por el hecho de que los paquetes enviados poseen una bandera SYN característica para establecer una conexión con alguna de ellas. Este escaneo lo está realizando a través del puerto de la NetBIOS (puerto 139).

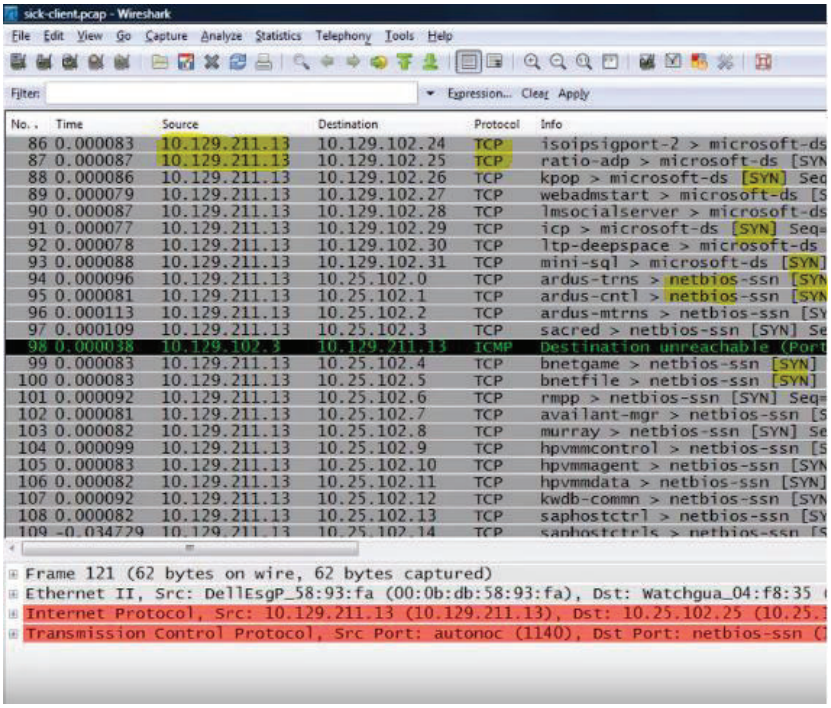


Figura 5.37. Escaneo de puertos por bot malicioso

Ahora bien, se ha llegado a un punto en el que el proceso de escaneo continúa con todas las direcciones que la comunicación IRC ha señalado, y como ejemplo en el paquete 98, se tiene que las respuestas a los intentos de conexión son “destino inalcanzable” lo cual le indica que el dispositivo posee un firewall activo o simplemente no existe. Este proceso continúa durante toda la captura de tráfico hasta que el atacante encuentre un host activo con el cual también pueda establecer conexión.

Se ha analizado el caso de este malware, y su mitigación es igualmente realizada en el caso de estudio número 1, lo cual consiste en indagar que es la página a la cual se está estableciendo conexión (bbjj.household.com), y el resultado nos indicará que tipo de malware se está enfrentando para así poder dar un tratamiento específico a este. El resultado obtenido con el browser se puede visualizar en la Figura 5.38. Buscando en qué consiste página maliciosa

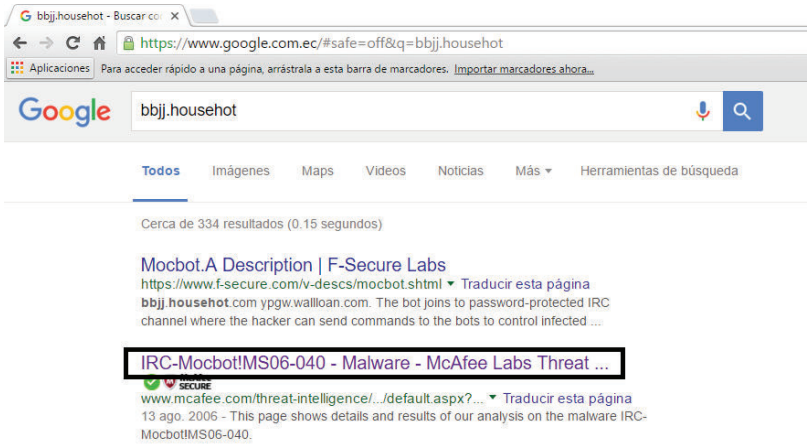


Figura 5.38. Buscando en qué consiste página maliciosa

Otra posibilidad es indagar directamente en la página de “VirusTotal” (ya mencionada en el primer caso de estudio), con la URL atacante (bbjj.household.com), y como se evidencia en el resultado estas es una página maliciosa como se puede observar en Figura 5.39. Resultado de VirusTotal a página atacante.

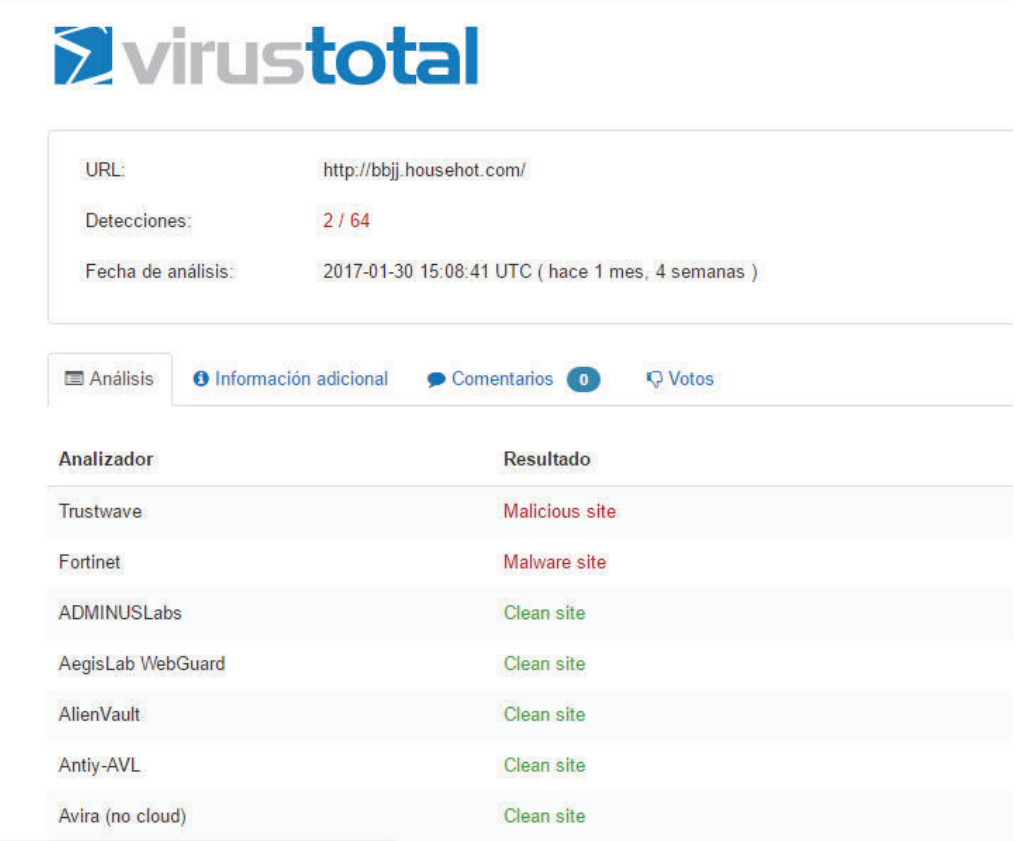


Figura 5.39. Resultado de VirusTotal a página atacante

5.1.2.3. Conclusiones

En conclusión, las amenazas más comunes en el tráfico de una red de área local son las siguientes:

- Arp Spoofing
- MAC Flooding
- Denegación de Servicio (DoS)
- DHCP Spoofing
- VLAN Hopping
- Malware

Una vez identificadas las características que debe cumplir el paso de la metodología "Identificación de la Amenaza" (definido en esta Sección 5.1.2), y de igual manera, identificadas las amenazas posibles mediante la herramienta de análisis de tráfico de red por medio de los pasos de "Captura" y "Análisis", ya es posible concluir las características del segundo formulario que se encuentra en el Anexo II y abarcan lo siguiente:

- Identificar la o las herramientas con las cuales se realizará el análisis de la red.
- Identificar las fuentes de amenaza humana en el tráfico de red, sean estos ataques deliberados o no intencionales [6, p. 14].
- Mantener actualizada la lista de amenazas ayudándose de: agencias de inteligencia, el Centro Federal de Respuesta a Incidentes de Computadora (FedCIRC) [73], reportes de seguridad mundiales [70], etc.

5.1.3. Análisis de Control

El tercer paso de la metodología es el análisis de control donde como su nombre mismo lo dice, se requiere analizar los controles implementados o que están próximos a implementarse por la organización para minimizar o eliminar la probabilidad de que una amenaza explote una vulnerabilidad [6]. Estas amenazas orientadas al tráfico de red fueron descritas en la Sección 5.1.2 [21].

Al hablar de probabilidad necesitamos una calificación verosímil que nos indique el porcentaje de que una vulnerabilidad pueda ser explotada por cada una de las amenazas descritas, es decir, necesitamos asociar cada una de las amenazas a un

porcentaje de probabilidad de ocurrencia. Para lograr esto se debe tener en cuenta los controles que se tienen implementados o que están próximos a implementarse en la organización para contrarrestar estos riesgos en el tráfico de red. Estos métodos de control son de dos tipos: técnicos y no técnicos [11].

- Controles técnicos: Hace referencia a hardware, software o firmware para controlar el tráfico de red (firewalls, proxys, antivirus, etc.).
- Controles no técnicos: controles de gestión o políticas de la organización para prevenir que el tráfico normal de la red se vea afectado.

5.1.3.1. Categorías de control

Los controles técnicos y no técnicos encontrados se clasifican también en controles preventivos y de detección según corresponda a cada control [6]. Los controles preventivos son los que inhiben los intentos de violar la política de seguridad en torno al tráfico de red estos incluyen controles tales como control de acceso, cifrado y autenticación. Por otro lado los controles de detección nos advierten de violaciones o intentos de violaciones de la política de seguridad en torno al tráfico de red e incluyen métodos de detección de intrusiones a la red, detección de tráfico sospechoso, detección de autenticaciones ilegales, auditoría a la red etc.

5.1.3.2. Conclusiones

Cabe tomar en cuenta que la herramienta de la cual nos estamos ayudando para el análisis de tráfico de red (Wireshark) no interfiere en esta fase de la metodología, a menos de que la organización la tenga implementada como control. En este caso, se la registra únicamente como control de la organización pero no se la utiliza para análisis de tráfico.

Una vez definido lo que se debe realizar en esta fase, se puede concluir las características que tendrá este formulario en esta fase las cuales se encuentran en el Anexo III, y son:

- Listado de los controles técnicos y no técnicos implementados en la organización.
- Listado de los controles técnicos y no técnicos próximos a implementarse en la organización.
- Categorización de los controles siendo estos preventivos o de detección.

5.1.4. Determinación de la Probabilidad

Para lograr determinar la probabilidad de que una fuente de amenaza logre explotar una cierta vulnerabilidad, se debe en primer lugar determinar la naturaleza de la vulnerabilidad. Para esto se requiere determinar un listado de vulnerabilidades del sistema que puedan ser explotadas por una fuente de amenaza.

Para determinar la o las vulnerabilidades, se puede implementar los siguientes métodos de obtención de datos:

- Documentación referente a evaluaciones de riesgo realizadas con anterioridad en el sistema de TI.
- Reportes de: auditoría, anomalías de sistema, revisión de seguridad, pruebas de sistema, reportes de evaluación.
- Listado de vulnerabilidad existentes. Puede ser obtenida por ejemplo de la NIST NVD (Base de Datos Nacional del Instituto Nacional de Estándares y Tecnología).
- Avisos de seguridad globales como los que anuncia la FedCIRC (Centro Federal de Respuesta a Incidentes Informáticos).
- Avisos de proveedores.
- Reportes de equipos de respuesta a incidentes/emergencias.
- Sistema de análisis de software de seguridad.

Además, otra forma fundamental que nos permite identificar vulnerabilidades es realizar una prueba al sistema informático, y aquí es donde la Sección 5.1.2 anteriormente realizada es clave, ya que al momento de identificar las amenazas en el sistema y realizar el paso de “Análisis” del tráfico capturado, estamos también evaluando al sistema para determinar las vulnerabilidades que este tiene. Este listado de vulnerabilidades encontradas se debe incluir también en el listado final de vulnerabilidades existentes.

Estas pruebas que se realizan con la herramienta se denominan “pruebas de evaluación de seguridad” la cual prueba la eficacia de los controles implementados en el sistema. Además se puede complementar esta prueba con una “prueba de penetración” que evalúan al sistema en torno a que tanto puede resistir a los intentos deliberados para burlar la seguridad del sistema. Una vez ya determinado el listado de vulnerabilidades existentes. Se puede ya establecer una calificación a la probabilidad

de que una vulnerabilidad pueda ser explotada por una fuente de amenaza asociada ya que se cuenta con los tres factores esenciales que son:

- Fuente de amenaza
- Naturaleza de la vulnerabilidad
- Existencia y efectividad de los controles existentes

La probabilidad de que una potencial vulnerabilidad pueda ser explotada por una fuente de amenaza puede ser descrita como alta, media, o baja. Cada uno de los significados de probabilidad se describe en la Tabla 5.1. Descripción de la Probabilidad.

Tabla 5.1. Descripción de la Probabilidad

Probabilidad	Descripción
Alta probabilidad	Los controles implementados son ineficaces para evitar que la vulnerabilidad sea explotada por una fuente de amenaza altamente motivada.
Media probabilidad	Existen controles que pueden impedir que una vulnerabilidad pueda ser explotada pero la amenaza igualmente está motivada.
Baja probabilidad	La fuente de amenaza carece de motivación o capacidad, o los controles están listos para prevenir o impedir que una vulnerabilidad sea explotada.

5.1.4.1. Conclusiones

Con la definición de “Determinación de la Probabilidad”, ya se puede concluir lo que debe poseer el formulario respectivo para esta fase el cual se encuentran en el Anexo IV:

- Listado de vulnerabilidades propensas a ser explotadas por una fuente de amenaza.
- Fuente de obtención de cada una de las vulnerabilidades.
- Probabilidad de ocurrencia asociada a cada una de las amenazas de la lista en base a los controles existentes, controles próximos a implementarse y vulnerabilidades encontradas.

5.1.5. Análisis de Impacto

El siguiente paso esencial en la medición del nivel de riesgo es determinar el impacto adverso resultante cuando una amenaza explota exitosamente una vulnerabilidad. Para esto se requiere tener en claro:

- La misión del Sistema.
- Los procesos y datos críticos. (El valor del sistema y los datos de importancia para la organización).
- La sensibilidad del sistema y los datos. (Hace referencia a que tan sensibles son los datos y el sistema para la continuidad de los procesos).

Esta información puede ser obtenida de la documentación que maneja la organización, pero previa gestión del acceso a la documentación (la gestión al acceso de activos se encuentra en la Sección 5.1.1. [6].

Esta información que se obtenga puede incluir el informe de evaluación de criticidad de activos o el análisis de impacto al negocio (BIA) el cual prioriza el nivel de impacto y lo asocia con los activos de información de la organización y se basa en una evaluación cualitativa o cuantitativa de la sensibilidad y criticidad de dichos activos. Una evaluación de criticidad de activos identifica y prioriza los activos de información de organización sensibles, en este caso activos relacionados con el tráfico de red crítico en la organización (hardware, software, sistemas, servicio, etc.)

En caso de no existir documentación, se puede determinar la sensibilidad del sistema y los datos en función del nivel de protección necesario para mantener disponibles, íntegros y confidenciales los datos y el sistema. Esta acción debe ser realizada por los propietarios del sistema y de la información, por lo tanto, al analizar el impacto, el enfoque apropiado es entrevistar al sistema y al propietario de la información en torno al nivel de protección existente.
De lo descrito se puede definir que el impacto adverso de un evento de seguridad puede describirse en términos de pérdida o degradación de la seguridad en torno a la: integridad, disponibilidad y confidencialidad del sistema y de los datos.

- **Pérdida de Integridad**

La integridad del sistema y de los datos se refiere al requisito de que la información esté protegida contra modificaciones inadecuadas. La integridad se pierde si se

realizan cambios no autorizados en los datos o en el sistema informático por actos intencionales o accidentales. Si no se corrige la pérdida de integridad del sistema o de los datos, el uso continuo del sistema contaminado o los datos dañados podrían resultar en imprecisiones, fraudes o decisiones erróneas. Además, la violación de la integridad puede ser el primer paso en un ataque exitoso contra la disponibilidad del sistema o la confidencialidad. Por todas estas razones, la pérdida de integridad reduce la seguridad de un sistema informático.

- **Pérdida de Disponibilidad**

Si un sistema de misión crítica de TI (importante para las operaciones críticas de la organización) no está disponible para sus usuarios finales, la misión de la organización puede verse afectada. La pérdida de funcionalidad del sistema y de su eficacia operativa, podría dar como resultado una pérdida de tiempo productivo, impidiendo así que los usuarios finales desempeñen sus funciones en el sistema.

- **Pérdida de Confidencialidad**

La confidencialidad de datos y del sistema se refiere a la protección de la información contra la divulgación no autorizada. El impacto de la divulgación no autorizada de información confidencial puede desde poner en peligro la seguridad nacional hasta la divulgación de la Ley de Privacidad de los datos. La divulgación no autorizada, imprevista o no intencional podría resultar en pérdida de confianza en la organización, poner en vergüenza a la organización o tomar acciones legales contra la organización.

El impacto se puede medir cualitativamente y/o cuantitativamente dependiendo de que se esté analizando, por ejemplo si se habla de pérdida de ingresos en la organización, costo de reparación en los sistemas, o costo de reposición de algún equipo; hablamos de un impacto cuantitativo.

Por otro lado si se trata, por ejemplo, de pérdida de confianza del público, pérdida de credibilidad de la organización o daño a una organización de interés; no se puede dar una medida específica por lo cual se debe describir en términos de impacto alto, medio o bajo; cada una descrita en la Tabla 5.2. Descripción del Impacto.

Tabla 5.2. Descripción del Impacto

Impacto	DESCRIPCIÓN
Alto Impacto	Se determina un alto impacto cuando una vulnerabilidad al ser explotada resulta en la pérdida con un altísimo costo de los principales activos tangibles o recursos; puede violentar, dañar o impedir la misión, reputación o interés de una organización.
Mediano Impacto	En el mediano impacto al explotar una vulnerabilidad, puede resultar en una perdida costosa de activos tangibles o recursos; puede además violentar, dañar o impedir la misión, reputación o interés de una organización pero no al nivel de un alto impacto.
Bajo Impacto	Se denomina como bajo impacto si al explotar una vulnerabilidad resulta en la pérdida de bajo costo de algunos activos o recursos tangibles o puede afectar notablemente en la misión, reputación, o interés de la organización.

5.1.5.1. Impactos Cualitativos vs. Activos Cuantitativos

Un impacto cualitativo tiene la ventaja de poder priorizar el riesgo e identificar áreas que requieren un inmediato mejoramiento en manejo de las vulnerabilidades, y su desventaja es que no es posible establecer una medida exacta de la magnitud del impacto por lo que dificulta un análisis costo-beneficio de los controles recomendados.

En el análisis cuantitativo la ventaja principal es el hecho de que provee una medida de la magnitud del impacto y esto facilita el análisis costo-beneficio de los controles recomendados, pero a su vez, al establecer una medida numérica puede no darnos una clara idea clara de que tan “fuerte” es el impacto por lo que se requiere en base a un rango numérico interpretar al impacto cuantitativo de una forma cualitativa.

Finalmente, para determinar efectivamente el impacto se requiere tomar en cuenta algunos factores los cuales son:

- Una estimación de la frecuencia con la que una fuente de amenaza explote una vulnerabilidad durante cierto periodo.
- Un costo aproximado para cada ocurrencia de la fuente de amenaza explotando una vulnerabilidad.

- Realizar un análisis subjetivo del impacto relativo del ejercicio de una amenaza sobre una vulnerabilidad por cada proceso, y en base a esto obtener un valor ponderado del impacto y categorizarlo.

5.1.5.2. Conclusiones

En esta fase de la metodología, lo que se pretende es determinar qué tan crítico sería el hecho de que una fuente de amenaza explotara una vulnerabilidad a lo cual estamos denominando impacto. Una vez analizado el impacto, se puede concluir las características que tendrá el formulario en esta fase el cual se encuentra en el Anexo V:

- Listado de los procesos del negocio relacionados al sistema de TI que se está analizando, y una valoración del impacto que se tendría en el caso de que estos procesos se vean afectados por una vulnerabilidad al ser explotada por una fuente de amenaza.
- Adjuntar al formulario los documentos de análisis de impacto del negocio y documentación referente al impacto de la organización.

5.1.6. Determinación del Riesgo

En esta fase de la metodología se evalúa finalmente el nivel de riesgo para el sistema de TI. Esta fase metodológica de “Determinación del Riesgo” hace match con el paso de “Documentación” para el análisis de tráfico de red, ya que junto con esta fase se presentará todos los formularios realizados con los hallazgos encontrados en el proceso metodológico y se presentará una recomendación o recomendaciones para el posterior tratamiento de estos riesgos. Esta documentación generada ayudará a la organización para poder planificar un plan de tratamiento de riesgo a futuro en un plazo establecido internamente con lo que se logrará mitigar el riesgo dentro de la organización.

Esta fase de determinación del riesgo se la realiza para cada par amenaza - proceso, y se puede expresar como función de:

- La probabilidad de que una fuente de amenaza determinada intente explotar una vulnerabilidad dada.
- La magnitud del impacto en los procesos del sistema en caso de que una fuente de amenaza tenga éxito explotando la vulnerabilidad.

- La adecuación de los controles de seguridad planificados o existentes para mitigar el riesgo.

Para lograr medir el riesgo se debe desarrollar una matriz de medición del riesgo como la encontrada en la Sección 5.1.6.1.

5.1.6.1. Matriz de medición del riesgo

Para determinar el riesgo se debe multiplicar las calificaciones asignadas para la probabilidad de amenaza (alto, medio, bajo) y el impacto en los procesos (alto, medio, bajo). La Tabla 5.3. Matriz para determinación del riesgo, muestra mediante una matriz 3x3 cómo se pueden determinar las calificaciones globales de riesgo basándose en la probabilidad de ocurrencia de una amenaza y el impacto de la misma. Si se requiere una especificación mayor (mayor granularidad), se puede establecer una matriz 4x4 o 5x5 incluyendo probabilidades de ocurrencia “muy altas” o “muy bajas”, las cuales pueden ser determinadas en términos subjetivos.

A estas calificaciones del impacto y de la probabilidad, se les puede asignar un valor numérico el cual se asociará a un valor cualitativo. Por ejemplo:

- Para la probabilidad de ocurrencia de cada amenaza se asigna un nivel de 1.0 para Alto, 0.5 para Medio, 0.1 para Bajo.
- Para el nivel de impacto se asigna los valores de 100 para Alto, 50 para Medio y 10 para Bajo.

Todo esto se observa también en la Tabla 5.3. Matriz para determinación del riesgo

Tabla 5.3. Matriz para determinación del riesgo

Impacto / **Probabilidad de Amenaza**	**BAJO (10)**	**MEDIO (50)**	**ALTO (100)**
BAJO (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10
MEDIO (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
ALTO (1.0)	Bajo 10 x 1 = 10	Medio 50 x 1 = 50	Alto 100 x 1.0 = 100

La Tabla 5.3. Matriz para determinación del riesgo maneja una escala de:

- Alto: >50 a 100
- Medio: >10 a 50
- Bajo: 1 a 10

Esta evaluación también presenta acciones que los directivos de la organización deber tomar para cada riesgo, lo cual se puede visualizar en la Tabla 5.4. Acciones necesarias a seguir por cada riesgo.

Tabla 5.4. Acciones necesarias a seguir por cada riesgo

Determinación del Riesgo	Acciones Necesarias para combatir cada riesgo.
ALTO	Si un riesgo se determina con una calificación de "Alto", se deben realizar con urgencia medidas correctivas. El sistema puede seguir operando pero un plan de acciones correctivas se debe poner en marcha lo antes posible
MEDIO	Si un riesgo se determina con una calificación de "Medio", se deben realizar medidas correctivas. El sistema opera con normalidad pero se requiere realizar un plan de acciones correctivas dentro de un periodo de tiempo razonable establecido por la organización.
BAJO	Si un riesgo se determina con una calificación de "Bajo", el sistema operará con normalidad, y la autoridad de aprobación designada de la organización debe determinar si se requieren tomarán acciones correctivas, o decidir si se acepta el riesgo.

Pueden existir riesgos resultantes con valores menores a 1 los cuales se considerarán como "insignificantes". Estos riesgos se deben considerar en una lista separada para que en el siguiente análisis y evaluación de riesgos sean tomados en cuenta ya que tanto su impacto y/o la probabilidad de ocurrencia de la amenaza pueden incrementar su valor.

5.1.6.2. Conclusiones

En esta sección de la metodología se evalúa finalmente el riesgo, el cual se lo obtiene a partir de la probabilidad de ocurrencia de que una vulnerabilidad sea explotada por una amenaza, y la determinación del impacto que generaría en los procesos del sistema esta vulnerabilidad al ser explotada por una fuente de amenaza.

De esto se obtiene que las características del formulario en esta fase deban ser:

- Matriz de Riesgo del sistema informático en base a la determinación de la probabilidad de ocurrencia de cada una de las amenazas descritas, y su impacto posible a la organización.
- Análisis del riesgo de cada uno de los procesos informáticos categorizados en "Altos", "Medios" o "Bajos".
- Recomendación general a seguir para tratamiento del riesgo.

El formulario de esta fase de la metodología se encuentra en el Anexo VI.

5.2. Aplicación del Modelo Propuesto a un Caso de Estudio

5.2.1. Presentación del Caso de Estudio

Durante los cuatro capítulos anteriores, se ha abarcado todo lo concerniente al modelo propuesto, con la cual se pretende realizar una efectiva evaluación del riesgo mediante la aplicación de formularios creados a partir de un análisis metodológico de normas existentes para el análisis y evaluación del riesgo, así como también el análisis del tráfico de una red de área local (LAN).

Para lograr plantear el modelo propuesto, se partió del levantamiento del sustento teórico necesario para la evaluación de riesgo. Posteriormente se realizó un estudio de marcos de referencia para la evaluación del riesgo, y se realizó un análisis comparativo de los marcos de referencia con el fin de obtener las mejores prácticas para evaluar el riesgo. Después se realizó un estudio comparativo entre herramientas para el análisis del tráfico de red, con la cual se obtuvo la mejor herramienta y los pasos requeridos para realizar un análisis del tráfico de red. Con las mejores prácticas de la metodología y los pasos requeridos para realizar el análisis de tráfico de red, se realizó un match metodología-análisis de tráfico, con lo cual se logró finalmente realizar los formularios que nos permiten analizar y evaluar el sistema de TI mediante el análisis de tráfico optimizando el tiempo de ejecución.

Resta ahora validar el modelo propuesto con la aplicación los formularios creados. Estos formularios se aplicaron en una institución muy importante a nivel nacional en donde se maneja una gran cantidad de procesos propensos al riesgo. Cabe mencionar que la metodología se aplicó en una LAN como se tenía propuesto realizar, y el alcance del análisis abarca una LAN y no trasciende a la red metropolitana (MAN) o la red amplia de la organización (WAN).

La institución en la cual se aplicó el modelo propuesto es la **DIGERCIC – Dirección General de Registro Civil, Identificación y Cedulación** más conocido como el Registro Civil del Ecuador. Esta institución pública existente desde 1901 tiene como objetivo la identificación integral de personas y de registro de hechos y actos civiles en el Ecuador. Institución que se encuentra a cargo del Director General del Registro Civil – Ing. Jorge Oswaldo Troya Fuertes.

La DIGERCIC está formada por 5 coordinaciones principales que la conforman, las cuales se pueden evidenciar en la Figura 5.40. Organigrama de la DIGERCIC [74]. La “Coordinación General de Tecnologías de la Información y Comunicación” formada por un personal de 54 personas a nivel del país, es el lugar donde brindó la apertura para aplicar el modelo propuesto, más específicamente en la “Dirección de Infraestructura y Operaciones de TI” ubicado en la “Matriz del Registro Civil” al norte de Quito.

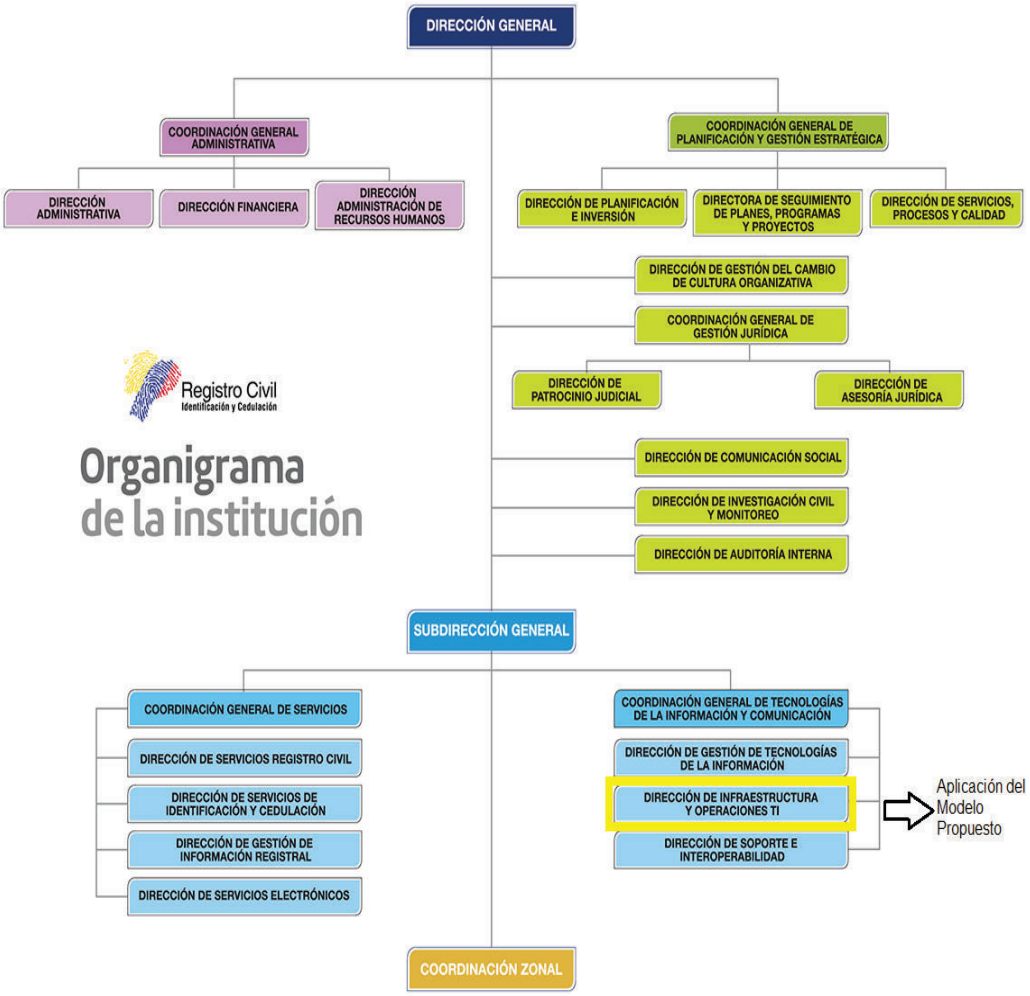


Figura 5.40. Organigrama de la DIGERCIC

Para acceder a la Institución se gestionó el permiso con el "Director General del Registro Civil" – Ing. Jorge Troya, y se socializó el modelo propuesto con el "Coordinador General de Tecnologías de la Información y Comunicación" – Ing. Manuel Rodríguez, el cual direccionó a la "Dirección de Infraestructura y Operaciones de TI" para aplicar el modelo propuesto en uno de los sistemas más críticos de la organización "Sistema Magna – Sistema Principal de Cedulación".

Las personas de apoyo asignadas en la organización para aplicar el modelo propuesto fueron el Ing. Mauricio Correa (Analista de Gobierno de TI), y el Ing. Fernando Daqui (Analista de Redes).

En síntesis, el caso de estudio se simplifica en: Análisis y evaluación de riesgo del Sistema Magna de Cedulación en la Matriz de la DIGERCIC mediante el análisis de tráfico de red.

5.2.2. Aplicación Metodológica

En esta sección se menciona el resultado de la aplicación del modelo propuesto en el caso de estudio, y se lo categoriza por formularios aplicados. Cabe mencionar que por aspectos de seguridad institucional y el acuerdo de confidencialidad con la institución, varios aspectos se describen de forma general sin profundizar en detalles.

5.2.2.1. Aplicación del Formulario 1 – Caracterización del Sistema

Al llenar el primer formulario aplicado al caso de estudio que se encuentra en el Anexo VII, se pudo identificar aspectos generales y específicos de la institución pública necesarios para realizar el análisis y evaluación de riesgo. Se cumple con lo requerido en la metodología que como en su nombre lo dice, es caracterizar al sistema de TI lo cual se encuentra en la Sección 5.1.1.

Al haber aplicado el primer formulario:

1. Se respondió la pregunta de dónde se realizará el análisis y evaluación de riesgo. El formulario contiene información referente a la institución por área y departamento, así como también información a nivel físico en donde se hará la captura de datos.
2. Se definió el alcance que tendrá la aplicación del análisis en el sistema Magna (sistema principal de cedulación de la DIGERCIC) con el fin de saber que se ha cumplido con el objetivo requerido para el análisis y evaluación de riesgo.
3. Se describió también el personal dentro de la institución al cual se solicitó el acceso a los activos de información, así como también el personal de apoyo para realizar el análisis.
4. Se reconoció la infraestructura de la red LAN de la institución, sobretodo en la cual viaja el tráfico concerniente al sistema Magna de cedulación.
5. Se analizó la infraestructura de red, y apoyado del analista de redes se determinó el mejor lugar y la mejor forma de realizar el paso de “plan de análisis” para la captura de tráfico de red, con lo cual se determinó que la mejor opción sería utilizando un puerto espejo o port mirroring descrito en la Sección 5.1.1.1.2.

6. Se procedió a configurar un puerto espejo del puerto de salida de todas las VLAN de módulos de cedulación en el switch de piso el cual se conecta directamente al switch core (switch principal), para ahí colocar la máquina con la herramienta para captura de paquetes. La configuración del puerto espejo se observa en la Figura 5.41. Port Mirroring en Switch de VLAN de Cedulación.

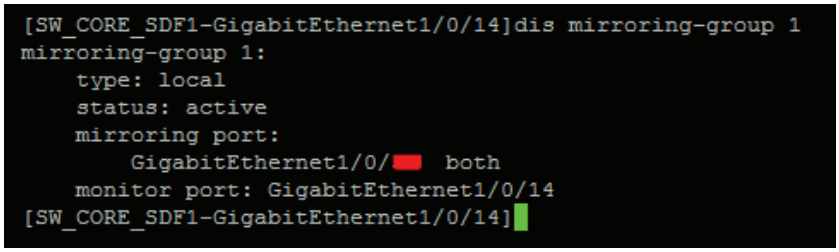


Figura 5.41. Port Mirroring en Switch de VLAN de Cedulación

5.2.2.2. Aplicación del Formulario 2 – Identificación de la Amenaza

El segundo formulario aplicado al caso de estudio se encuentra en el Anexo VIII. En esta fase, el objetivo fundamental fue encontrar amenazas en el tráfico de red capturado que es lo que establece esta fase de la metodología según lo mencionado en la Sección 5.1.2. Para esto partimos del punto anterior donde logramos ubicar la máquina para realizar la captura de tráfico. En esta máquina tenemos el sniffer de red con el cual se procedió a la captura del tráfico.

Al haber aplicado el segundo formulario:

1. Se determinó la herramienta para la captura y análisis de tráfico de red. Siguiendo el análisis comparativo de herramientas realizado en la Sección 4.4, la herramienta seleccionada fue Wireshark.
2. Se realizó la captura de tráfico de red directamente en el “puerto mirroring” configurado en la sección anterior. Este puerto se ubicó físicamente en el switch de piso donde se encuentran los módulos de cedulación en un área restringida. Esto se evidencia en la Figura 5.42. Captura de tráfico de módulos de cedulación.

Figura 5.42. Captura de tráfico de módulos de cedulación

3. Se capturó una cantidad aproximada de 2 millones de paquetes de tráfico de red equivalente a un archivo de 1.5 GB de espacio según se puede evidenciar en la Figura 5.43. Tráfico capturado en módulos de cedulación.

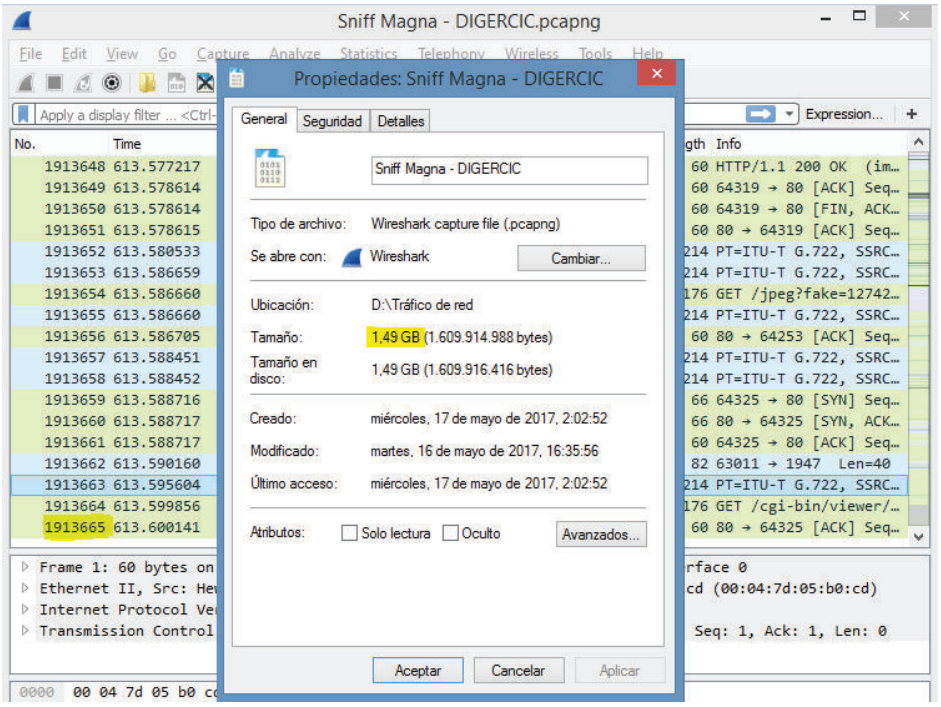


Figura 5.43. Tráfico capturado en módulos de cedulación

4. Se analizaron los paquetes capturados con Wireshark en base a lo descrito en la Sección 5.1.2 y en base a Wireshark Expert Information (módulo de la propia herramienta) con lo que se concluyó lo siguiente:

5.2.2.2.1. Detección de ARP Spoofing

Después de analizar el tráfico de red en torno a amenazas “ARP Spoofing” según lo descrito en la Sección 5.1.2.2.1, se concluyó que el único dispositivo que resuelve más de una dirección IP con una misma MAC es el “SwitchCore” (switch principal) de la matriz según se evidencia en la Figura 5.44. ARP de SwitchCore, por lo cual no existen amenazas de este tipo.

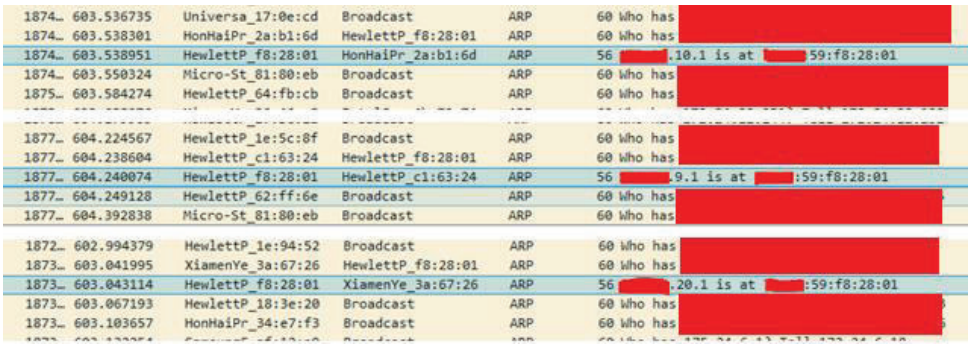


Figura 5.44. ARP de SwitchCore

5.2.2.2.2. Detección de MAC Flooding

Igualmente, después de analizar el tráfico en torno a amenazas “MAC Flooding” en base a la Sección 5.1.2.2.2, se identificó que no existen paquetes TCP o UDP mal formados que contengan direcciones MAC falsas que traten de inundar a los switch de piso o al “SwitchCore” de la institución. Llos únicos paquetes TCP mal formados corresponden a datos reenviados por paquetes ACK según se evidencia en la Figura 5.45. Reenvío de Paquetes ACK. Todas las MAC correspondían al tráfico de red normal de la institución, por lo concluyente no existen amenazas de este tipo.

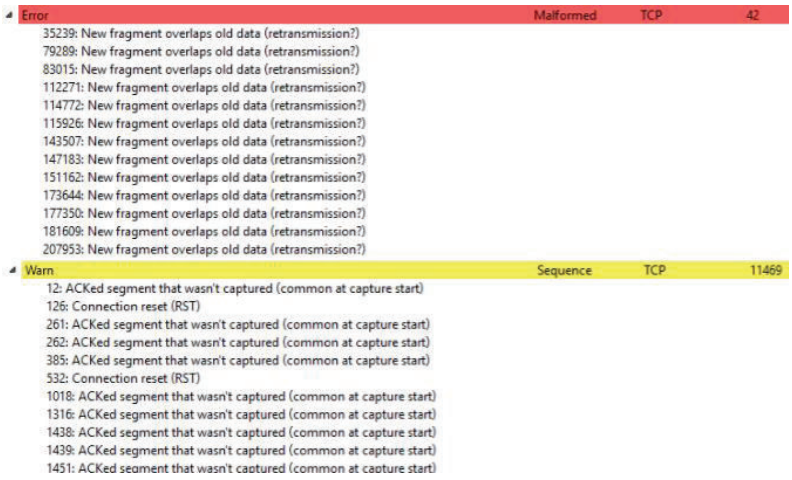


Figura 5.45. Reenvío de Paquetes ACK

5.2.2.2.3. Detección de Denegación de Servicio (DoS)

En torno a ataques de “Denegación de Servicio”, en base a lo descrito en la Sección 5.1.2.2.3, la conexión “three way handshake” de las tramas TCP se realizan con normalidad dentro de los equipos de la institución, exceptuado por una gran cantidad de paquetes ACK que se pierden en la negociación de tres pasos lo que responde a una alerta de Wireshark, posiblemente por un mala configuración o antigüedad de algunos switch de piso según lo comentado por el analista de redes de la institución. Esto conlleva a una posible vulnerabilidad del sistema lo cual se registra posteriormente, entonces, no existe amenazas de tipo DoS pero existe una vulnerabilidad de paquetes ACK perdidos que se registrará posteriormente, esto igualmente se puede evidenciar en la Figura 5.45. Reenvío de Paquetes ACK.

5.2.2.2.4. Detección de DHCP Spoofing

En la detección de ataques de “DHCP Spoofing”, según la Sección 5.1.2.2.4, todos los paquetes se enrutan a las direcciones correctas ya que se maneja un direccionamiento estático en la LAN de la institución, por lo que un ataque por DHCP no surgiría efecto, y por ende no se encontró ataques de este tipo.

5.2.2.2.5. Detección de MAC Flooding

Para detectar ataques “VLAN Hopping”, siguiendo lo establecido en la Sección 5.1.2.2.5, se analizó los paquetes DTP para la detección de máquinas intrusivas que se quieran hacer pasar como switch. Analizando estos paquetes, se concluyó que todo el tráfico se estaba enrutando correctamente por los switch Cisco de piso con las direcciones MAC auténticas según se evidencia en Figura 5.46. Captura de paquetes DTP, por lo cual no se evidenció un “VLAN Hopping” por suplantación de switch. Se analizó también los paquetes ICMP para detectar un etiquetado doble de paquetes, pero se encontraban correctamente formados sin doble encabezado, esto se sustenta igualmente en el hecho de que no existen otros dispositivos ajenos a la red detectados en el tráfico capturado, por lo que no se encontró ataques de este tipo.

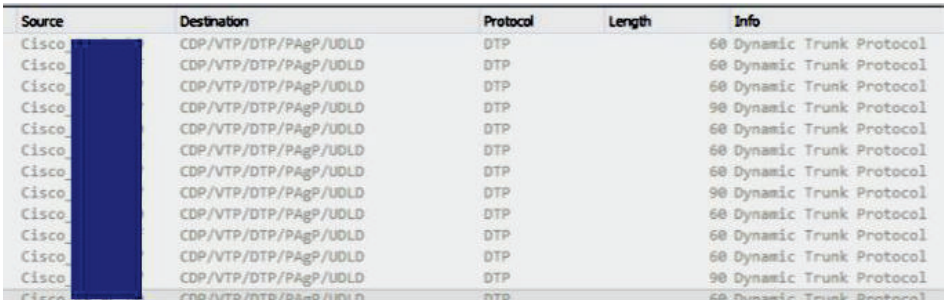


Figura 5.46. Captura de paquetes DTP

5.2.2.2.6. Detección de Malware

Para la detección de Malware, se sigue las pautas descritas en la Sección 5.1.2.2.6, el objetivo es identificar tráfico anómalo o software malicioso en el tráfico de la LAN. Para esto se decidió en primer lugar, indagar sobre los archivos que están siendo descargados en los host de la LAN y quienes los están descargando. Cabe recordar que se está analizando todas las VLAN de los módulos de cedulación del sistema Magna; aquí se detectó:

a. **Malware “ldr.php” de página “hzmksreiuojy.in” y página “hzmksreiuojy.nl”:** Según se evidencia en la Figura 5.47. Detección de malware "ldr.php" de páginas atacantes con Wireshark, se detectó tráfico malicioso de las páginas web “hzmksreiuojy.in” y “hzmksreiuojy.nl”, las cuales están descargando un archivo llamado “ldr.php”, este archivo es un malware potencialmente peligroso que afecta directamente a browsers mediante pop-ups, redireccionando a páginas para descargas de virus y más malware. Este archivo genera además spam para

engañar y sugerir compra de productos para supuestamente deshacerse del virus. Puede recopilar información sensible, ayudar al atacante a infiltrarse remotamente, bajar considerablemente la velocidad del sistema, e incluso estropearlo completamente [75].

Se puede evidenciar el informe de “VirusTotal” de la página “hzmksreiuojy.in”, al igual de la localización de este atacante en la Figura 5.48. Informe VirusTotal de página "hzmksreiuojy.in". También se puede evidenciar el informe de “VirusTotal” de la página “hzmksreiuojy.nl”, al igual de la localización del otro atacante en la Figura 5.49. Informe VirusTotal de página "hzmksreiuojy.nl". A pesar de que es el mismo ataque, se realiza de dominios diferentes localizado en ciudades diferentes.

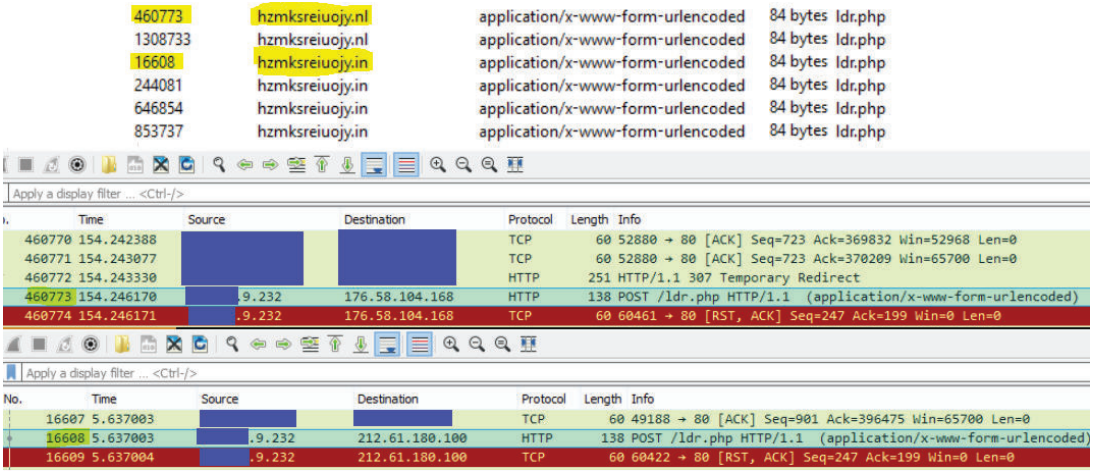


Figura 5.47. Detección de malware "ldr.php" de páginas atacantes con Wireshark

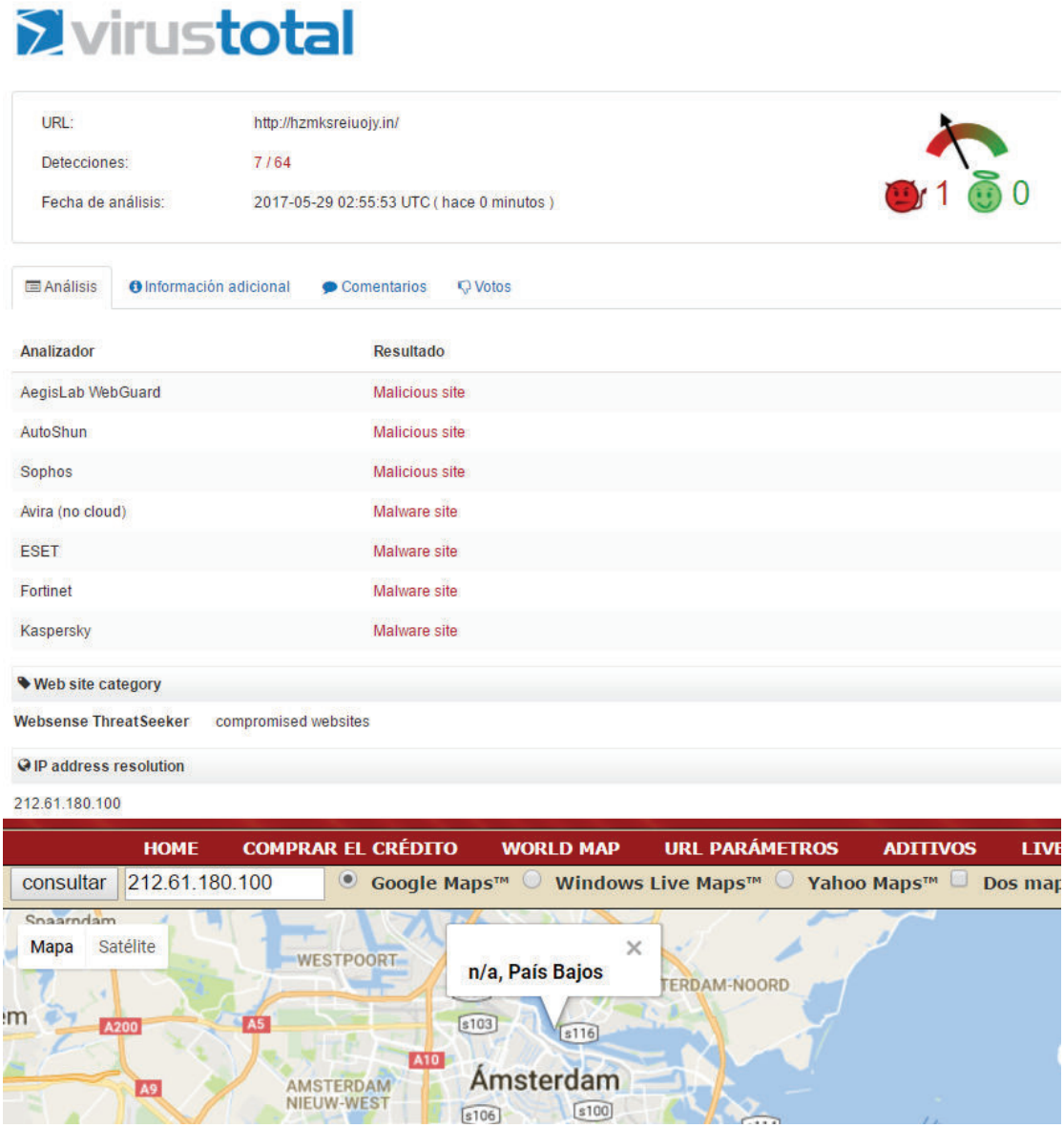


Figura 5.48. Informe VirusTotal de página "hzmksreiuojy.in"

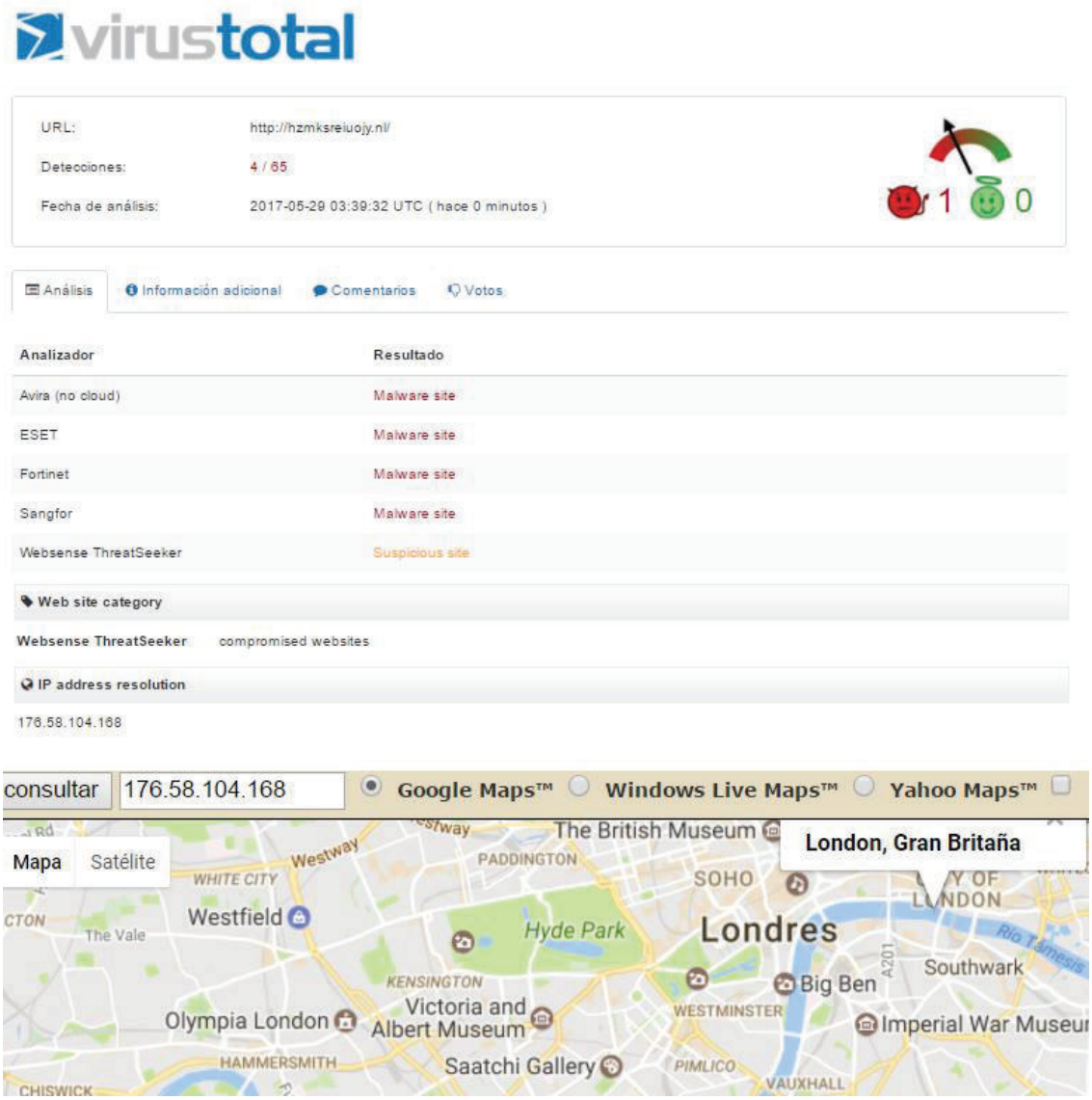


Figura 5.49. Informe VirusTotal de página "hzmksreiuojy.nl"

b. **Tráfico sospechoso de páginas "ocsp.digicert.com", "ocsp.entrust.net", "ocsp.comodoca.com":** Según se evidencia en la Figura 5.50. Detección de tráfico sospechoso OCSP con Wireshark, el segundo caso de malware encontrado se sustenta en varias páginas de análisis de dominios las cuales señalan que las páginas señaladas descargan posibles virus que afectan a los navegadores, mostrando pop-ups no deseados, redirección a páginas sospechosas, cambiando el motor de búsqueda de los navegadores, y generando spam a correos [76]. Analizando los dominios de estas páginas, se identificó que se encuentran localizados en dos diferentes países (EE.UU., Inglaterra), a pesar de que este tráfico podría estar respondiendo a una seguridad del proveedor de Internet

utilizando el protocolo OCSP (Protocolo comúnmente utilizado para mantener seguridad de servidores y recursos de red) [77]. En vista de que este tráfico sigue siendo un tráfico de red extraño y mientras no se descarte completamente como inofensivo se lo debe tratar como tráfico malicioso. Además existe ya un tráfico OCSP que proviene de la página “tj.symcd.com”, dominio que se encuentra registrado por Symantec el cual brinda mayor confianza, ya que podría ser el tráfico OCSP real. Este tráfico se evidencia en la Figura 5.51. Detección de tráfico OCSP de "tj.symcd.com" con Wireshark.

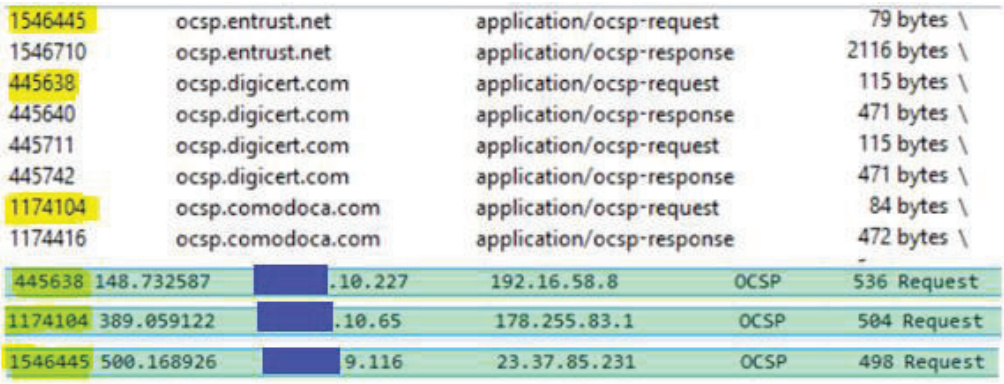


Figura 5.50. Detección de tráfico sospechoso OCSP con Wireshark

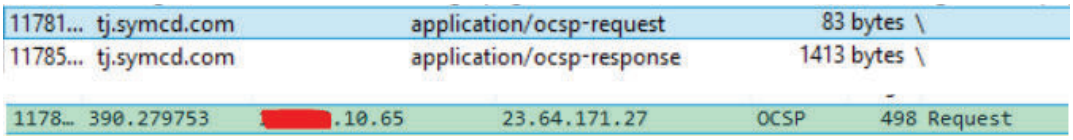


Figura 5.51. Detección de tráfico OCSP de "tj.symcd.com" con Wireshark

El reporte de “VirusTotal” para las tres páginas analizadas nos señala que no existen detecciones peligrosas, pero el reporte de usuarios es negativo en los tres casos según se evidencia en la Figura 5.52. Informe "VirusTotal" de páginas sospechosas.

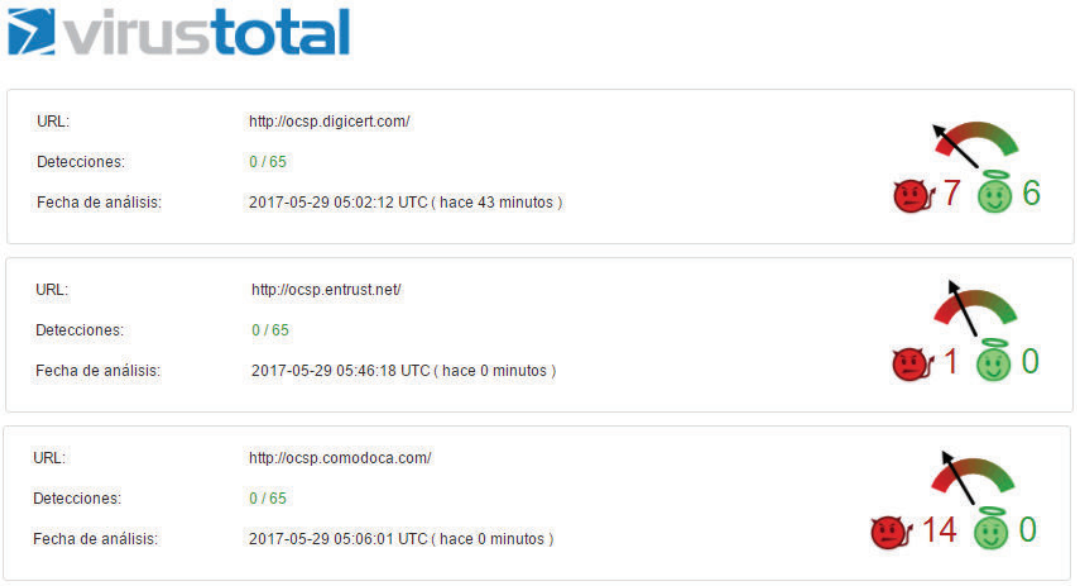


Figura 5.52. Informe "VirusTotal" de páginas sospechosas

c. **Malware "order.php" de página "disorderstatus.ru":** Según se evidencia en la Figura 5.53. Detección de malware "order.php" de "disorderstatus.ru" con Wireshark, se detectó tráfico malicioso de la página web "disordersatus.ru", la cual está descargando un archivo llamado "order.php". Este archivo es un adware peligroso que afecta directamente a browsers. Creado con el fin de recopilar información confidencial de usuarios, trabaja igualmente con pop-ups redireccionando a páginas para descargas de spyware y más malware, genera ventanas emergentes no deseadas y recopila información no autorizada, puede incluso generar inestabilidad en el sistema por lo que se considera una amenaza de alto riesgo [78]. El informe de "VirusTotal" de la página "disoderstatus.ru" nos muestra claramente que es una página de malware en base al análisis realizado. Esto se puede visualizar en la Figura 5.54. Informe "VirusTotal" de página "disorderstatus.ru".

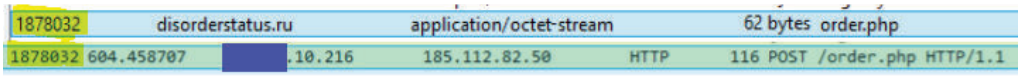


Figura 5.53. Detección de malware "order.php" de "disorderstatus.ru" con Wireshark

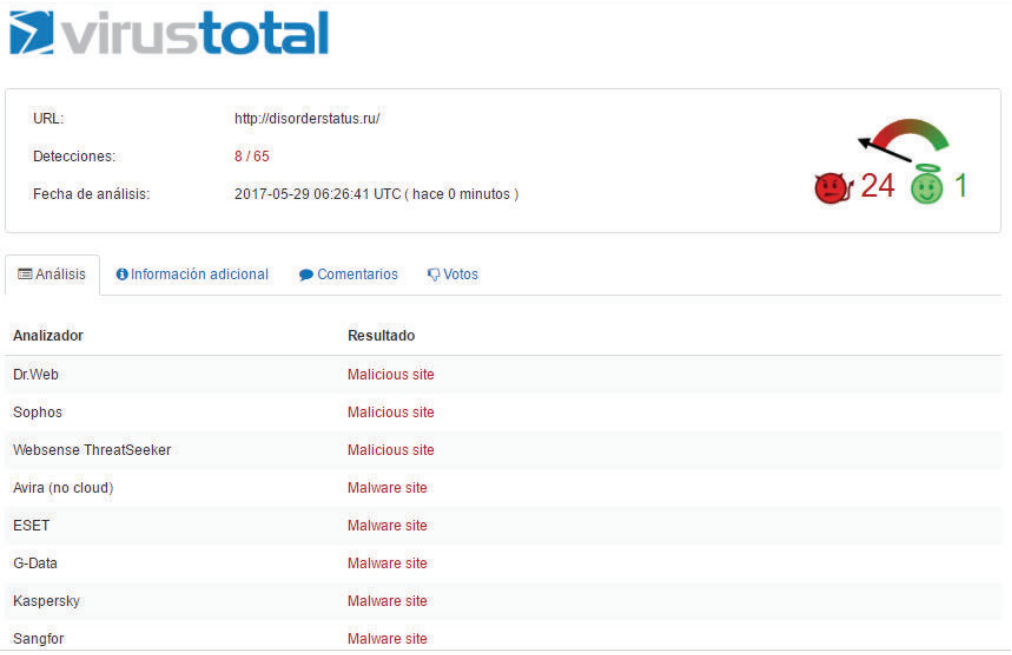


Figura 5.54. Informe "VirusTotal" de página "disorderstatus.ru"

d. **Intento de páginas atacantes en host local para establecer conexión a internet:** Se realizó también una búsqueda de páginas sospechosas mediante el análisis de tráfico DNS. De esto se obtuvo que existe un host infectado en la red el cual trata de acceder a las páginas “hzmksreiuojy.biz”, “hzmksreiuojy.ru”, “hzmksreiuojy.com”, “hzmksreiuojy.in”, “hzmksreiuojy.nl”, estos dos últimos ya como amenazas en la red según lo analizado en esta sección. Estas páginas tratan de ser accedidas mediante el servidor de dominios 8.8.4.4, Estos intentos de conexión se pueden observar en la Figura 5.55. Detección mediante Wireshark de intentos de conexión de páginas atacantes.

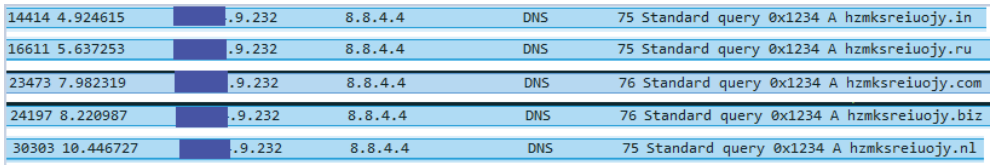


Figura 5.55. Detección mediante Wireshark de intentos de conexión de páginas atacantes

5. Después de identificado todas las amenazas existentes en el tráfico de red capturado, se pretendió simular un ataque interno en la institución desde un módulo de cedulación. Esto se realizó con el objetivo de probar al sistema contra un ataque de los descritos en la Sección 5.1.2.2. Para este ataque controlado, se eligió el ataque “ARP Spoofing”, ya que era el menos influyente en la red y la continuidad de los procesos de la organización. Para esto en primer lugar se eligió una de las VLAN de cedulación y se colocó la herramienta dentro de esta con una IP de módulos (vale la pena mencionar que para poder conocer una IP dentro de la VLAN, un usuario final de los módulos debería realizar un escaneo de IP’s para poder realizar el ataque, o a su vez atacar desde su misma dirección IP. También se puede dar el caso en que una persona externa pueda implementar Ingeniería Social con el fin de acceder a esta información, luego poder acceder a un puerto y realizar el ataque, pero esto es menos probable).

e. **ARP Spoofing (Ataque Simulado):** Para generar este ataque nos basamos en la Sección 5.1.2.2.1, además se utilizó la herramienta Cain y Abel para realizar el ataque [58]. Ya con el equipo atacante con IP dentro de la VLAN, se procedió a realizar el ARP Spoofing a otro equipo de la red, y se empezó la captura de tráfico con el atacante envenenando al otro host de la red. Esto se evidencia en la Figura 5.56. ARP Spoofing con Cain y Abel.

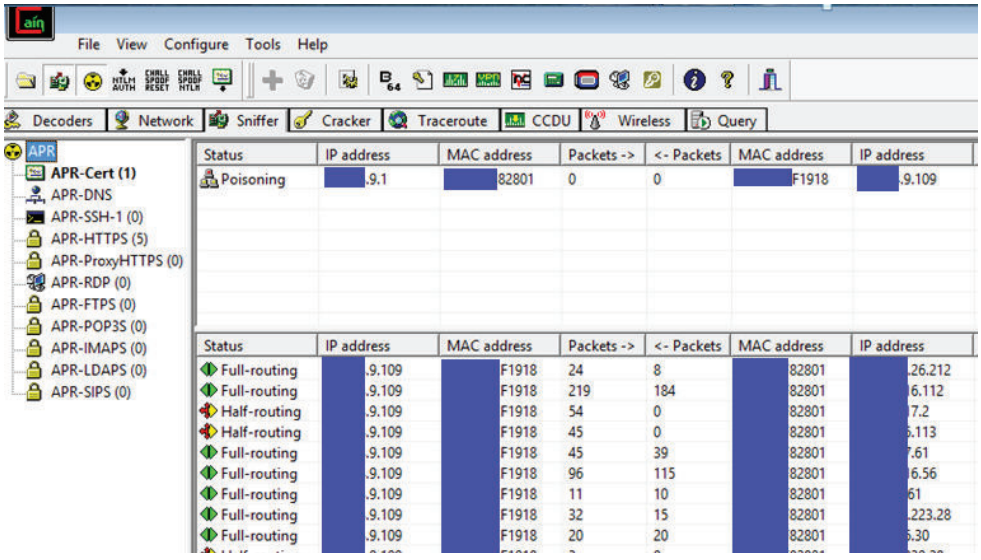


Figura 5.56. ARP Spoofing con Cain y Abel

El ataque se realizó con éxito ya que el atacante logró acceder a todos los datos del host envenenado. Y el tráfico capturado respondió a lo esperado según lo descrito en la Sección 5.1.2.2.1. Esto se puede evidenciar en la Figura 5.57. ARP Spoofing detectado con Wireshark en Ataque Simulado, en la cual vemos el IP del atacante haciendo un "Man in the Middle" haciéndose pasar por la puerta de enlace por lo que todos los paquetes del host atacado con dirección (X.X.9.109) se enrutan a través de este.

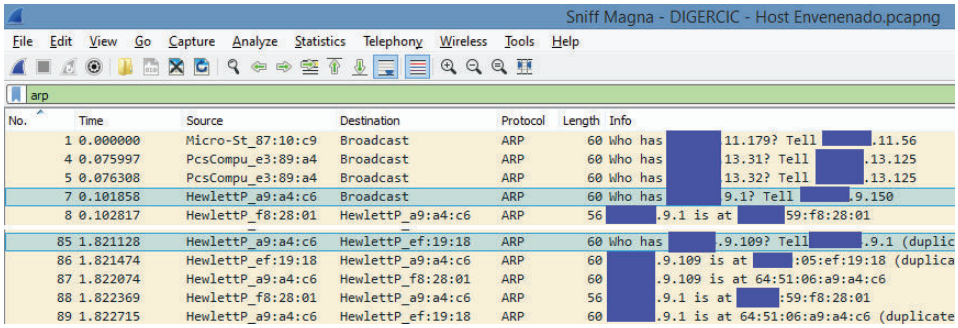


Figura 5.57. ARP Spoofing detectado con Wireshark en Ataque Simulado

Todo lo mencionado en esta Sección 5.2.2.2 se encuentra sintetizado en el Anexo VIII donde se evidencia el segundo formulario aplicado al caso de estudio.

5.2.2.3. Aplicación del Formulario 3 – Análisis de Control

Al llegar a este punto, ya se ha identificado las amenazas en la red del sistema de TI que se está analizando (Sistema "Magna"). Ahora llegamos a la fase del control donde se identificaron los controles establecidos en la institución para el "Sistema Magna" según lo descrito en la Sección 5.1.3. Se debe recordar que se delimitó los controles únicamente para el sistema que se está analizando y no de toda la institución. Además cabe tomar en cuenta que existieron controles que al momento de categorizarlos en preventivos y de detección, aplicaron para ambos criterios por lo cual se los registró por separado con un identificador diferente. El formulario aplicado al caso de estudio de esta fase se encuentra en el Anexo IX.

Al aplicar este formulario:

1. Se registraron los controles técnicos implementados para el Sistema Magna mediante el método de entrevista al "Analista de Redes" y al "Líder de Unidad de Plataforma de Software" de la institución, con lo que se registró 10 hallazgos preventivos y 2 de detección.

2. Se registraron los controles NO técnicos implementados para el Sistema Magna mediante el método de entrevista al “Analista de Gobierno de TI”, el cual consultó varios aspectos al “Director de Infraestructura y Operaciones”, en esta categoría se registró 3 hallazgos preventivos y 3 de detección, entre políticas, códigos de buenas prácticas y auditorías.
3. Mediante método de entrevista al “Analista de Redes”, se registró los controles técnicos próximos a implementarse en la institución para el sistema “Magna”, además se solicitó el tiempo estimado en meses para la implementación de dicho control. En esta categoría se registró 2 hallazgos preventivos y 2 de detección.
4. Finalmente, mediante el método de entrevista igualmente al “Analista de Gobierno de TI”, se registró los controles NO técnicos próximos a implementarse en la institución para el sistema “Magna”, además se solicitó el tiempo estimado en meses para la implementación de dicho control. En esta categoría se registró 4 hallazgos preventivos y 2 de detección.

5.2.2.4. Aplicación del Formulario 4 – Determinación de la Probabilidad.

El formulario de determinación de la probabilidad aplicado al caso de estudio cuyo contenido se puede evidenciar en el Anexo X, tuvo como objetivo determinar cuál es la probabilidad que se materialicen las amenazas encontradas en la Sección 5.2.2.2. Esta probabilidad de ocurrencia de la amenaza categorizada en alta, medio, o baja, se determinó según los controles y vulnerabilidades existentes en el sistema “Magna”. Las acciones requeridas para la determinación de la probabilidad se encuentran en la Sección 5.1.4.

Al haber aplicado este formulario:

1. Se determinó las herramientas que nos ayudaron en el proceso de detección de vulnerabilidades para el sistema “Magna”, con las cuales se realizaron pruebas de análisis de tráfico al sistema y análisis de penetración. Se utilizó la herramienta “Wireshark” para el análisis de tráfico de red, “Cain y Abel” para realizar pruebas de penetración y Nmap para realizar un mapeo de la red. Se debe tomar en cuenta que mientras se ejerció el segundo formulario de detección de la amenaza, también se detectaron vulnerabilidades a la par, las cuales también fueron registradas en el siguiente paso.

2. Se determinó las vulnerabilidades del sistema “Magna” en base a la entrevista realizada al “Analista de Gobierno de TI”, al “Líder de la Unidad de Plataformas de Software”, al “Analista de Redes” y también mediante la utilización de las herramientas descritas en el paso 1.

   No existe documentación referente a vulnerabilidades del sistema de la organización, por lo que la información en torno a vulnerabilidades se la obtuvo únicamente mediante los métodos descritos anteriormente. La información brindada por el personal, fue obtenida mediante análisis internos realizados en el ejercicio de sus funciones por parte del personal de TI, y de los usuarios.

   Con todo esto se determinaron un total de 14 vulnerabilidades generales, mayormente relacionadas a la gestión técnica del sistema y tráfico de red. También se hallaron vulnerabilidades en torno a la falta de controles no técnicos, y también a la falta de aplicación de los controles no técnicos existentes en la institución por parte de los usuarios.

   Cabe mencionar que las vulnerabilidades se las ha descrito de la forma más general posible y que en el formulario hallado en base a esta sección no se encontrarán las vulnerabilidades detalladas explícitamente por seguridad y acuerdo de confidencialidad firmado con la institución.

3. Una vez determinadas las vulnerabilidades, se procedió al análisis de la probabilidad de ocurrencia de las amenazas encontradas en base a los controles establecidos o próximos a establecerse por la institución (descritos en el formulario 3), y las vulnerabilidades del sistema registradas en el segundo paso de este formulario, de lo que se concluyó que:
   - La amenaza A1 “Malware “ldr.php” de página “hzmksreiuojy.in” y página “hzmksreiuojy.nl”, en base a los controles descritos (8 técnicos y 3 no técnicos), y las vulnerabilidades encontradas (8 vulnerabilidades), tiene una probabilidad de ocurrencia: MEDIA.
   - La amenaza A2 “Tráfico sospechoso de páginas “ocsp.digicert.com”, “ocsp.entrust.net”, “ocsp.comodoca.com””, en base a los controles descritos (8 técnicos y 4 no técnicos), y las vulnerabilidades encontradas (8 vulnerabilidades), tiene una probabilidad de ocurrencia: BAJA.
   - La amenaza A3 “Malware “order.php” de página “disorderstatus.ru””, en base a los controles descritos (8 técnicos y 3 no técnicos), y las vulnerabilidades encontradas (8 vulnerabilidades), tiene una probabilidad de ocurrencia: MEDIA.

- La amenaza A4 “Intento de páginas atacantes en host local para establecer conexión a internet””, en base a los controles descritos (6 técnicos y 4 no técnicos), y las vulnerabilidades encontradas (8 vulnerabilidades), tiene una probabilidad de ocurrencia: BAJA.
- La amenaza A5 “ARP Spoofing (Ataque simulado)”, en base a los controles descritos (5 técnicos y 3 no técnicos), y las vulnerabilidades encontradas (10 vulnerabilidades), tiene una probabilidad de ocurrencia: ALTA.

5.2.2.5. Aplicación del Formulario 5 – Análisis de Impacto.

La aplicación del formulario de análisis de impacto aplicado al caso de estudio cuyo contenido se puede evidenciar en el Anexo XI, nos permitió evaluar el impacto en alto, medio o bajo que experimentaría el sistema, más específicamente los procesos del sistema al materializarse las amenazas. Esta fase de la metodología se encuentra descrita en la Sección 5.1.5.

Al realizar este formulario:

1. Se describió la forma en que se obtuvo la información en torno a la criticidad del sistema. La institución no posee documentación alguna en la cual se describa que tan crítico son los procesos del sistema, por lo cual, mediante el método de entrevista al “Analista de Gobierno de TI” y al “Analista de Plataformas de Software” y el documento de “Diagrama de Estados de Magna - Application State Machine” se determinó la criticidad de procesos.
2. Se realizó un análisis para determinar la criticidad de cada uno de los procesos descritos en el documento mencionado. Estos procesos del sistema (denominados “Estados” en la documentación) dan un total de 18 procesos del sistema, a los cuales se los categorizó en procesos muy crítico, críticos, y poco críticos en base a que tan influyentes son para el cumplimiento de la misión del sistema y cuáles son los controles establecidos para el control de estos procesos. Cabe mencionar que el criterio principal con el que se evaluó a cada uno de los procesos del sistema para determinar su criticidad, fue en evaluar que tan importante es cada uno de los procesos para cumplir con la misión general del sistema “Magna”, esta misión se encuentra descrita en el primer formulario.

3. Una vez descritos los procesos del sistema y categorizados por criticidad, se procedió a determinar el impacto adverso sobre cada uno de estos procesos al materializarse las amenazas, de lo que se determinó:
    - Los procesos: P9 (Validación de huellas - AFIS) y P13 (Implementación de seguridad en la fotografía - IPI), suman un total de 2 procesos de impacto: ALTO.
    - Los procesos: P1 (Estación de Captura), P3 (Registro en BDD Principal), P10 (Aprobación de la Aplicación), P14 (Solicitud de Impresión), P15 (Impresión), P16 (Registro de Impresión), P17 (Registro de Certificado), suman un total de 7 procesos de impacto: MEDIO.
    - Los procesos P2 (Recaptura), P4 (Validación por Abogado), P5 (Validación Offline), P6 (Redirección para Investigación), P7 (Investigación de Registro), P8 (Investigación de Impresión), P11 (Registro Rechazado), P12 (Registro de Terminación sin Impresión), P18 (Registro de Impresión de Certificado), suman un total de 9 procesos de impacto: BAJO

5.2.2.6. Aplicación del Formulario 6– Determinación del Riesgo.

Para finalizar se aplicó el formulario basado en la Sección 5.1.6 donde se determina el riesgo en base a toda la información recopilada. Este formulario se lo puede encontrar en el Anexo XII. Para determinar el riesgo se requirió el formulario 4 y 5 ya realizados anteriormente, y se los vinculó en base a la matriz de determinación del riesgo revisada anteriormente en la Tabla 5.3. **Matriz para determinación del riesgo**

Al realizar este formulario:

1. Se registró las 5 amenazas de la red encontradas y la probabilidad de ocurrencia de cada una de ellas, además se registró los 18 procesos del sistema Magna y el impacto adverso resultante cuando las amenazas se materializan. El riesgo se define como el impacto negativo neto del ejercicio de una amenaza, tomando en cuenta la probabilidad de ocurrencia como también el impacto a los procesos. Por lo tanto, el riesgo se define por cada par de probabilidad-impacto (amenaza-proceso), es decir 5 amenazas por 18 procesos dio un total de 90 resultados del riesgo, una copia de la matriz de riesgo resultante se puede observar en la Tabla 5.5. Resultado de Riesgo del Caso de Estudio.

Tabla 5.5. Resultado de Riesgo del Caso de Estudio

Impacto / Probabilidad de Amenaza		P2	P4	P5	P6	P7	P8	P11	P12	P18	P1	P3	P10	P14	P15	P166	P17	P9	P13
		10	10	10	10	10	10	10	10	10	50	50	50	50	50	50	50	100	100
A2	0,1	1	1	1	1	1	1	1	1	1	5	5	5	5	5	5	5	10	10
A4	0,1	1	1	1	1	1	1	1	1	1	5	5	5	5	5	5	5	10	10
A1	0,5	5	5	5	5	5	5	5	5	5	25	25	25	25	25	25	25	50	50
A3	0,5	5	5	5	5	5	5	5	5	5	25	25	25	25	25	25	25	50	50
A5	1	10	10	10	10	10	10	10	10	10	50	50	50	50	50	50	50	100	100

En esta tabla se visualiza el resultante final del análisis y evaluación de riesgo del sistema “Magna” mediante el análisis del tráfico de la red. Como se puede observar la mayor cantidad de riesgos son bajos (un total de 63), existe una menor cantidad de riesgos medios (un total de 25) y finalmente una mínima cantidad de riesgos altos (un total de 2), sumando un total de 90 valores finales.

De la Tabla 5.5. Resultado de Riesgo del Caso de Estudio, se pudo obtener los datos necesarios para generar un solo valor ponderado con el cual se evalúe al sistema en porcentaje. Para esta acción se requirió identificar el peor de los escenarios posibles en la evaluación del riesgo del sistema, la cual se daría cuando las 5 amenazas tuviesen una probabilidad de ocurrencia máxima, es decir, tuviesen el valor de 1; y el impacto adverso en los 18 procesos del sistema fuera alto, es decir, con el valor de 100. Esto generaría una matriz de evaluación del riesgo solo con valores altos (100). Sumando todos los valores altos de 100 en la matriz nos darían un resultante de 9000 que equivaldría al riesgo máximo posible en el sistema, es decir, un riesgo total del 100%. Ahora analizando el caso real resultante en el que el existen valores de riesgo altos, medios y bajos se podría sumar el total de valores de riesgo resultantes y mediante una regla de tres determinar el riesgo total del sistema. Todo lo mencionado se puede visualizar en la Tabla 5.6. Peor de los casos en la matriz y la Tabla 5.7. Caso real en la matriz de.

Tabla 5.6. Peor de los casos en la matriz de riesgo del sistema “Magna”

Categorización del Riesgo	Riesgo = Probabilidad de Ocurrencia X Impacto	Cantidad de Resultados por valores	TOTAL
ALTO	100	90	**9000**

Tabla 5.7. Caso real en la matriz de riesgo del sistema "Magna"

Categorización del Riesgo	Riesgo = Probabilidad de Ocurrencia X Impacto	Cantidad de Resultados por valores	TOTAL
BAJO	1	18	18
BAJO	5	32	160
BAJO	10	13	130
MEDIO	25	14	350
MEDIO	50	11	550
ALTO	100	2	200
		TOTAL	**1408**

De la Tabla 5.6. Peor de los casos en la matriz de riesgo del sistema **"Magna**, y la Tabla 5.7. Caso real en la matriz de riesgo del sistema "**Magna** podemos realizar la regla de tres sobre el peor de los casos la cual que quedaría así:

$$\text{Porcentaje de Riesgo del Sistema} = \frac{1408 \times 100}{9000} = 15{,}64\%$$

De lo que en conclusión se puede determinar que en base a la probabilidad de ocurrencia de la amenaza y el impacto en los procesos del sistema de TI, el porcentaje total de riesgo en el sistema "**Magna**" es de 15.64%. Este valor no se registró en este formulario, pero puede ser presentado como una observación al momento de presentar la documentación final.

2. Se registró la cantidad de riesgos altos, medios y bajos en la Tabla 5.4. Acciones necesarias a seguir por **cada riesgo** (del formulario en el Anexo XII), en la cual consta la acción general requerida a realizar según el resultado obtenido de riesgo.

3. Toda la documentación recopilada en los 6 formularios fue socializada con la institución (como paso final), lo que permitirá brindar a la institución una visión más clara para poder establecer un plan de tratamiento del riesgo donde se combatan las amenazas existentes en la red local, y se coordine una mejor

gestión de los procesos del sistema para reducir el impacto y lograr mitigar el riesgo.

5.2.3. Conclusiones y recomendaciones del Caso de Estudio

En el tiempo que implicó todo el proceso de levantamiento de información (una semana aproximadamente) para realizar el análisis y evaluación del riesgo del "Sistema Magna", se pudo evidenciar que la coordinación de TIC de la DIGERCIC conformada por solo 56 personas a nivel nacional (mayormente desarrolladores), tiene a su cargo uno de los sistemas más críticos de todo el país como es el sistema de cedulación. A pesar de su reducido personal, han venido innovando e implementando mejoras en el sistema, no solo a nivel tecnológico, sino en la gestión que abarca todo el proceso crítico de cedulación.

En base al análisis y evaluación de riesgo realizado al "Sistema Magna" (sistema principal de cedulación) mediante el análisis de tráfico de red, se determinó un riesgo relativamente bajo del 15,64%. Cabe recalcar que este porcentaje hubiese sido mucho menor si no se hubiese realizado la simulación de ataque a la red el cual fue efectuado con el fin de realizar una prueba de penetración del sistema y evaluar el sistema en torno a ataques generados en su LAN, y en eso precisamente es lo que se debe recalcar. Los controles técnicos y no técnicos implementados en la institución contrastan con las amenazas de la red, pero las vulnerabilidades deben ser mitigadas para que el contraste sea predominante.

La institución debe priorizar la ingeniería social ya que una gran cantidad de las vulnerabilidades y amenazas son validadas por los propios usuarios del sistema. Se debe priorizar también en el monitoreo del usuario final mediante el análisis periódico del tráfico de la red para mitigar los riesgos existentes, enfocarse en las amenazas que tengan una probabilidad de ocurrencia alta, y en los procesos más críticos del sistema, para garantizar la continuidad de la organización. Fomentar la aplicación de políticas establecidas ya que muchas veces quedan "en el simple papel". Y finalmente, se recomienda a la institución la implementación de un mayor personal, ya que la gestión, control, análisis, desarrollo, evaluación y monitoreo de un sistema tan crítico como es el de identificar a cada persona de un país, es algo que requiere mucha atención.

CONCLUSIONES Y RECOMENDACIONES

A continuación se redactan las conclusiones y recomendaciones finales del proyecto.

Conclusiones

Realizar el análisis y evaluación de riesgo de un sistema de TI es uno de los procesos más importantes en las prácticas de una organización. Mediante la ejecución de una metodología e implementando una herramienta para el análisis de tráfico de red, es posible estimar el riesgo existente en los procesos críticos y no críticos del sistema, todo esto sustentado en base a un análisis de las amenazas, vulnerabilidades y controles existentes dentro la organización. En torno a esto, se realizó un análisis y evaluación de riesgo al sistema de TI denominado “Magna”, y se lo evaluó en torno a amenazas del tráfico de red. Este análisis fue realizado en base a un estudio comparativo de metodologías de evaluación de riesgo y de herramientas para análisis de tráfico con lo que se logró satisfactoriamente proponer un modelo para obtener los riesgos del sistema y cumplir con los objetivos propuestos.

El levantamiento teórico de activos de información es una tarea esencial al momento de realizar un análisis de tráfico en la red de un sistema de TI. Este sustento teórico debe asegurar los conocimientos claros y necesarios para brindar un escenario seguro sobre la actividad que se va a realizar. De igual manera, el análisis de tráfico de red en un sistema es una tarea de vital importancia que debe ser ejecutada con el fin de evitar pérdidas graves en los activos de información. Este análisis debe seguir un orden coherente en base a un plan establecido, y debe ser llevado a cabo periódicamente con el fin de garantizar seguridad, disponibilidad y confiabilidad en el sistema, en base a este criterio, se realizó un levantamiento de sustento teórico en el que se establecieron los pasos requeridos para hacer un análisis de tráfico de red y para poder identificar tanto amenazas como vulnerabilidades.

El proceso de implementación de una metodología para analizar y evaluar el riesgo conlleva la necesidad del estudio de la misma para poderla aplicar, además involucra el proceso de investigación con el cual se determine las prácticas que se involucrarán en el proceso de evaluación. Todo esto involucra tiempos que muchas veces la organización no los asigna, ya que requieren una respuesta rápida y eficaz que les permita evaluar su sistema en un menor tiempo. Para esto, el modelo propuesto presenta seis formularios que permitieron vincular el estudio comparativo para análisis

y evaluación de riesgo, y el proceso de análisis de tráfico de la red, y con esto de una forma sencilla evaluar el riesgo de un sistema de TI optimizando el tiempo requerido para el proceso de evaluación.

Finalmente, la aplicación de un modelo propuesto a un caso de estudio es un proceso apropiado si se requiere justificar la validez del modelo, por esto, para validad el planteamiento propuesto de realiza un análisis y evaluación de riesgo de seguridad informática a través del análisis del tráfico de la red utilizando formularios creados a partir de un estudio metodológico. Se aplicó el modelo propuesto a un caso de estudio realizado en una institución pública de la cual se obtuvo los resultados esperados, ya que se logró satisfactoriamente abarcar todos las fases planteadas en la evaluación y finalizar con la obtención del riesgo del sistema de TI analizado, todo este proceso en un tiempo corto que satisfizo el objetivo propuesto de la optimización del tiempo.

Recomendaciones

Previo a la aplicación del método propuesto de realizar la evaluación del riesgo mediante el uso de los formularios, se recomienda realizar la correcta gestión para el acceso a los activos requeridos en el levantamiento de la información del sistema. Este proceso debe realizarse socializando el objetivo de la metodología con el coordinador del área o jefe del departamento, detallando claramente los recursos a los cuales se va a solicitar acceso. Al tener un correcto acceso a los activos, se puede facilitar el proceso de evaluación del sistema y aminorar tiempos en la implementación de este. Se debe recordar que se está manejando información sensible para la organización, por lo que se debe también realizar el correcto resguardo de activos para evitar causar algún problema.

Al aplicar los formularios propuestos para realizar el proceso de evaluación del riesgo, puede que genere una complicación al momento de requerir mayores casilleros para llenar algún parámetro en los mismos formularios (amenazas, vulnerabilidades, procesos, etc.), por lo que si se requiere mayor espacio se recomienda copiar la página final de cada formulario y complementar con la información requerida, este es un proceso válido que debe aplicarse en cualquier formulario que requiera mayor espacio para el llenado de datos.

Finalmente, la aplicación de los formularios creados para análisis y evaluación de riesgo puede resultar un proceso sencillo, pero identificar las amenazas mediante el análisis de tráfico puede que no resulte tanto, más si no se es especialista en redes o seguridad. Es por esto que es recomendable si se requieren identificar amenazas en la LAN guiarse en la sección de “Identificación de la Amenaza” de este trabajo de titulación, o a su vez directamente en el Internet detallar los síntomas que experimenta el sistema, ya que páginas de seguridad informática de grandes empresas tienen información valiosa con procesos descritos para la detección de amenazas o vulnerabilidades mediante el análisis de la red.

REFERENCIAS

[1] M. Stott, «ARCNET works,» 1998. [En línea]. Available: http://www.arcnet.com/resources/HistoryATA.pdf. [Último acceso: 18 02 2016].

[2] Textos Científicos, «DIFERENCIAS ENTRE ETHERNET Y IEEE 802.3,» 22 02 2006. [En línea]. Available: http://www.textoscientificos.com/redes/ethernet/ethernet-vs-ieee8023. [Último acceso: 18 02 2016].

[3] IEEE, «ISO/IEC 27005:2011,» 01 06 2011. [En línea]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742. [Último acceso: 18 02 2016].

[4] Textos Científicos, «CONTROL DE ACCESO AL MEDIO IEEE 802.3 CSMA/CD,» 22 02 2006. [En línea]. Available: http://www.textoscientificos.com/redes/ethernet/control-acceso-medio-csma-cd. [Último acceso: 18 02 2016].

[5] Directorate General for Administrative Modernisation, Procedures and Promotion of e-Government, «MAGERIT – version 3.0, Methodology for Information Systems Risk Analysis and Management,» 07 2014. [En línea]. [Último acceso: 21 03 2017].

[6] A. G. A. F. NIST - Gary Stoneburner, «Risk Management Guide for Information Technology Systems,» 07 2002. [En línea]. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. [Último acceso: 01 04 2016].

[7] Techopedia Inc., «Network Traffic Analysis,» 2015. [En línea]. Available: https://www.techopedia.com/definition/29976/network-traffic-analysis. [Último acceso: 19 02 2016].

[8] D. Benchimol, Redes Cisco, Banfield: Gradi S.A., 2010, p. 320.

[9] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, «MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» 10 2012. [En línea]. Available: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html. [Último acceso: 20 03 2017].

[10] ASIS International and British Standars Institution, «Organization Resilience:

Security, Preparedness, and Continuity Managment System-Requirements with Guidance for Use,» 12 03 2009. [En línea]. Available: https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf. [Último acceso: 05 03 2017].

[11] J. Sosa, «Análisis de Riesgos - Estándares para la administración de riesgos,» 27 01 2012. [En línea]. Available: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf. [Último acceso: 05 03 2017].

[12] Y. H. a. K. S. Amril Syalim, «Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide,» [En línea]. Available: https://pdfs.semanticscholar.org/1fe9/dae2ddaa3b145b99a98d7bbd918b1f820d74.pdf. [Último acceso: 05 03 2017].

[13] ENISA - European Network and Information Security Agency, «Threat and Risk Management - Literature,» [En línea]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/literature. [Último acceso: 05 03 2017].

[14] SIGEA, «Estándares para evaluar riesgos de seguridad de la información,» 24 06 2013. [En línea]. Available: https://www.sigea.es/estandares-para-evaluar-riesgos-de-seguridad-de-la-informacion/. [Último acceso: 05 03 2017].

[15] A. A. Mohamed S. Saleh, «A new comprehensive framework for enterprise information security risk management,» King Saud University, 14 02 2011. [En línea]. Available: http://ac.els-cdn.com/S2210832711000287/1-s2.0-S2210832711000287-main.pdf?_tid=aae30968-059e-11e7-8933-00000aacb35d&acdnat=1489156648_26fbd6fd621256eb82b10b18e9d14c41. [Último acceso: 09 03 2017].

[16] R. A. M. Y. Palaniappan Shamala, «A conceptual framework of info structure for information security risk assessment (ISRA),» 2013. [En línea]. Available: http://ac.els-cdn.com/S221421261300029X/1-s2.0-S221421261300029X-main.pdf?_tid=889338b0-059e-11e7-9ee7-00000aab0f26&acdnat=1489156591_fd2b70f530c930635a8fef261efecdab. [Último acceso: 10 03 2017].

[17] S. F. H. M. A. S. Mohamed Ghazouani, «Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk,» 10 2014. [En

línea]. Available: http://research.ijcaonline.org/volume103/number8/pxc3899155.pdf. [Último acceso: 09 03 2017].

[18] Y. H. K. S. Amril Syalim, «Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide,» 05 06 2009. [En línea]. Available: http://ieeexplore.ieee.org/abstract/document/5066554/. [Último acceso: 10 03 2017].

[19] J. D. C. V. Jose Manuel Matalobos Veiga, «Análisis de Riesgos de Seguridad de la Información,» 05 2009. [En línea]. Available: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf. [Último acceso: 09 03 2017].

[20] D. Pacheco, «Propuesta de un Plan de Contingencia de TI para la Empresa Logiciel,» 02 2016. [En línea]. Available: http://bibdigital.epn.edu.ec/bitstream/15000/15030/1/CD-6841.pdf. [Último acceso: 09 03 2017].

[21] P. D. G. NIST - Rebecca M. Blank, «Guide for Conducting Risk Assessments,» 09 2012. [En línea]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf. [Último acceso: 01 04 2016].

[22] CERT - Software Engineering Institute, «OCTAVE,» Carnegie Mellon UniversitY, 2017. [En línea]. Available: http://www.cert.org/resilience/products-services/octave/index.cfm. [Último acceso: 13 03 2017].

[23] J. F. S. L. R. Y. W. R. W. CERT - Richard A. Caralli, «The OCTAVE Allegro Guidebook, v1.0,» 05 2007. [En línea]. Available: https://acg6415.wikispaces.com/file/view/OCTAVE+Allegro+Method+v1.0.doc. [Último acceso: 13 03 2017].

[24] D. C. P. Pozo, «PROPUESTA DE UN PLAN DE CONTINGENCIA DE TI PARA LA EMPRESA LOGICIEL,» 02 2016. [En línea]. [Último acceso: 21 03 2017].

[25] E. J. P. E. J. A. B. P. Ana Abril, «RISK ANALYSIS IN SECURITY OF INFORMATION,» 23 12 2013. [En línea]. Available: http://www.revistasjdc.com/main/index.php/rciyt/article/view/292/283. [Último acceso: 26 03 2017].

[26] Syngress, «Introducing Network Analysis,» 09 2013. [En línea]. Available: http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Introducing-Network-Analysis.pdf. [Último acceso: 27 03 2016].

[27] L. Chappell, Wireshark Network Analysis - 2nd Edition, San Jose - California

(USA): Chappell University, 2012.

[28] Protocol Analysis Institute, «Wireshark University,» 2017. [En línea]. Available: http://www.wiresharktraining.com/certification.html. [Último acceso: 29 03 2017].

[29] Wireshark Foundation, «Chappell University,» 2017. [En línea]. Available: https://www.chappellu.com/. [Último acceso: 28 03 2017].

[30] J. L. David Caraballo, «The IRC Prelude,» irchelp.org, 2014. [En línea]. Available: http://www.irchelp.org/irchelp/new2irc.html. [Último acceso: 22 02 2016].

[31] S. Dhar, «Sniffers basics and Detection,» [En línea]. Available: http://www.just.edu.jo/~tawalbeh/nyit/incs745/presentations/Sniffers.pdf. [Último acceso: 27 03 2016].

[32] J. Biswas, «An Insight in to Network Traffic Analysis using Packet Sniffer,» 05 2014. [En línea]. Available: http://research.ijcaonline.org/volume94/number11/pxc3895975.pdf. [Último acceso: 27 03 2017].

[33] R. Spangler, «Packet Sniffer Detection with AntiSniff,» 05 2003. [En línea]. Available: http://www.packetwatch.net/documents/papers/snifferdetection.pdf. [Último acceso: 28 03 2017].

[34] G. S. R. P. G. P. S. B. K. S. Dr. Charu Gandhi, «Packet Sniffer – A Comparative Study,» 05 2014. [En línea]. Available: http://www.ijcncs.org/published/volume2/issue5/p6_2-5.pdf. [Último acceso: 27 03 2017].

[35] A. Tabona, «The Top 20 Free Network Monitoring and Analysis Tools for Sys Admins,» 15 05 2015. [En línea]. Available: https://techtalk.gfi.com/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/. [Último acceso: 28 03 2017].

[36] J. Wallen, «Five free network analyzers worth any IT admin's time,» 29 01 2013. [En línea]. Available: http://www.techrepublic.com/blog/five-apps/five-free-network-analyzers-worth-any-it-admins-time/. [Último acceso: 28 03 2017].

[37] R. Grimes, «6 Network Protocol Analyzers,» 28 06 2004. [En línea]. Available: http://windowsitpro.com/hardware/6-network-protocol-analyzers. [Último acceso: 28 03 2017].

[38] I. Bansal, «5 BEST FREE NETWORK PACKET SNIFFER,» 16 01 2011. [En línea]. Available: http://www.ilovefreesoftware.com/16/featured/5-best-free-network-packet-sniffer.html. [Último acceso: 27 03 2017].

[39] CERT (SEI) - Software Engineering Institute, «Packet Sniffing with Wireshark and Tcpdump,» [En línea]. Available: http://science.hamptonu.edu/compsci/docs/iac/packet_sniffing.pdf. [Último acceso: 28 03 2017].

[40] Elseiver, «Introducing Netwok Analysis,» 09 2013. [En línea]. Available: http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Introducing-Network-Analysis.pdf. [Último acceso: 27 03 2017].

[41] A. Gupta, «3 free Packet Sniffing Tools for Windows,» 06 06 2016. [En línea]. Available: http://www.thewindowsclub.com/free-packet-sniffing-tools. [Último acceso: 28 03 2017].

[42] Wireshark, «Wireshark,» Wireshark Foundation, 29 12 2015. [En línea]. Available: https://www.wireshark.org/. [Último acceso: 19 02 2016].

[43] Wireshark Foundation, «Wireshark,» [En línea]. Available: https://www.wireshark.org/#. [Último acceso: 22 02 2016].

[44] Tcpdump / Libpcap, «Tcpdump/Libpcap,» 2017. [En línea]. Available: http://www.tcpdump.org/. [Último acceso: 27 03 2017].

[45] microOLAP, «MicroOLAP TCPDUMP for Windows® 4.5.1,» 2017. [En línea]. Available: https://www.microolap.com/products/network/tcpdump/. [Último acceso: 27 03 2017].

[46] Colasfot, «Capsa Free Network Analyzer,» 2017. [En línea]. Available: http://www.colasoft.com/capsa-free/. [Último acceso: 27 03 2017].

[47] INTECO-CERT, «ANÁLISIS DE TRÁFICO CON WIRESHARK,» 02 2011. [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf. [Último acceso: 23 02 2016].

[48] Shashank Singh (Cisco), «Catalyst Switched Port Analyzer (SPAN) Configuration Example,» 21 04 2014. [En línea]. Available: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html. [Último acceso: 23 02 2016].

[49] Microsoft, «Cear un puente de red,» [En línea]. Available: http://windows.microsoft.com/es-419/windows/create-network-bridge#1TC=windows-7. [Último acceso: 23 02 2016].

[50] Neil DuPaul (Veracode), «Man in the Middle (MITM) Attack,» Veracode, 2016. [En línea]. Available: http://www.veracode.com/security/man-middle-attack. [Último acceso: 23 02 2016].

[51] Riverbed Technology, «WinPcap,» 08 03 2013. [En línea]. Available: http://www.winpcap.org/. [Último acceso: 24 02 2016].

[52] WinPcap documentation, «Remote Capture,» 2007. [En línea]. Available: http://www.winpcap.org/docs/docs_40_2/html/group__remote.html. [Último acceso: 28 03 2017].

[53] Riverbed Technology, «SteelCentral™ Packet Analyzer Personal Edition,» Wireshark® Enhancement Product, [En línea]. Available: https://www.riverbed.com/mx/forms/trial-downloads/Try-Evaluate-Cascade-Shark-Virtual-Edition-30-Day-Trial-Offer.html. [Último acceso: 23 05 2017].

[54] C. Maynard, «Wireshark Tools,» 08 03 2017. [En línea]. Available: https://wiki.wireshark.org/Tools. [Último acceso: 26 05 2017].

[55] Nmap, «Nmap Security Scanner,» 2017. [En línea]. Available: https://nmap.org/. [Último acceso: 26 05 2017].

[56] Virginia University, «Address Resolution Protocol,» [En línea]. Available: http://www.cs.virginia.edu/~cs458/slides/module06-arpV2.pdf. [Último acceso: 24 02 2016].

[57] Ettercap Project, «Welcome to the Ettercap Project,» [En línea]. Available: http://ettercap.github.io/ettercap/. [Último acceso: 25 05 2017].

[58] M. Montoro, «Oxid.it - Cain,» [En línea]. Available: http://www.oxid.it/cain.html. [Último acceso: 24 05 2017].

[59] Fabio Semperboni (CiscoZine), «Protecting against MAC flooding attack,» 05 01 2009. [En línea]. Available: http://www.ciscozine.com/protecting-against-mac-flooding-attack/. [Último acceso: 22 02 2016].

[60] M. McDowell, «Understanding Denial-of-Service Attacks,» US-CERTT, 06 02 2013. [En línea]. Available: https://www.us-cert.gov/ncas/tips/ST04-015. [Último acceso: 25 02 2016].

[61] The TCP/IP Guide, «TCP Connection Establishment Process: The "Three-Way Handshake",» 20 09 2005. [En línea]. Available: http://www.tcpipguide.com/free/t_TCPConnectionEstablishmentProcessTheThree WayHandsh-3.htm. [Último acceso: 26 02 2016].

[62] Infosec Institute, «LOIC (Low Orbit Ion Cannon) – DOS attacking tool,» 20 12 2011. [En línea]. Available: http://resources.infosecinstitute.com/loic-dos-attacking-tool/. [Último acceso: 25 05 2017].

[63] R. B. -. T. Lab, «HOIC DDoS Analysis and Detection,» 27 01 2012. [En línea].

Available: https://www.trustwave.com/Resources/SpiderLabs-Blog/HOIC-DDoS-Analysis-and-Detection/. [Último acceso: 25 05 2017].

[64] Ubuntu documentation, «Dynamic Host Configuration Protocol (DHCP),» [En línea]. Available: https://help.ubuntu.com/lts/serverguide/dhcp.html. [Último acceso: 26 02 2016].

[65] Ettercap Project, « Ettercap Project,» 2017. [En línea]. Available: http://ettercap.github.io/ettercap/. [Último acceso: 20 05 2017].

[66] NetApp Support, «How VLANs work,» NetApp, 2015. [En línea]. Available: https://library.netapp.com/ecmdocs/ECMP1368834/html/GUID-EC1DBB08-1B51-4981-A8D9-29835FC0149B.html. [Último acceso: 02 03 2016].

[67] Cisco, «Dynamic Trunking Protocol (DTP),» [En línea]. Available: http://www.cisco.com/c/en/us/tech/lan-switching/dynamic-trunking-protocol-dtp/index.html. [Último acceso: 02 03 2016].

[68] Yersinia , «Yersinia,» [En línea]. Available: http://www.yersinia.net/index.htm. [Último acceso: 24 05 2017].

[69] CERT-UK, «An introduction to malware,» 2014. [En línea]. Available: https://www.cert.gov.uk/wp-content/uploads/2014/08/An-introduction-to-malware.pdf. [Último acceso: 10 03 2016].

[70] Symatec Corporation, «Internet Security Threat Report | Appendices,» 21 04 2016. [En línea]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-appendices-en.pdf?aid=elq_&om_sem_kw=elq_16822104&om_ext_cid=biz_email_elq_&elqTrackId=4d82501a2e9e465d9fd77442e0c22384&elqaid=2910&elqat=2. [Último acceso: 12 12 2016].

[71] CNNTech (Virginia Harrison and Jose Pagliery), «Nearly 1 million new malware threats released every day,» 14 04 2015. [En línea]. Available: http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/. [Último acceso: 10 03 2016].

[72] Toad, «Introducción a TCP/IP,» 02 2005. [En línea]. Available: http://www.um.es/docencia/barzana/DIVULGACION/INFORMATICA/Introduccion_a_TCPIP.pdf. [Último acceso: 18 03 2016].

[73] U.S. General Services Administration, «FedCIRC Selects Global Integrity to Augment Incident Response Effort,» GSA Newsroom., 23 02 2017. [En línea]. Available: https://www.gsa.gov/portal/category/21188. [Último acceso: 29 03

2017].

[74] Registro Civil - Identificación y Cedulación, «Organigrama de la Institución,» 04 02 2015. [En línea]. Available: https://www.registrocivil.gob.ec/?p=4308. [Último acceso: 25 05 2017].

[75] F. George, «Guide to Delete http://hzmksreiuojy.in/ldr.php Completely,» QuickRemoveVirus.com, 18 12 2015. [En línea]. Available: http://quickremovevirus.com/guide-to-delete-httphzmksreiuojy-inldr-php-completely/. [Último acceso: 27 05 2017].

[76] l. Nightwatcher, «Remove ocsp.digicert.com virus (How to remove ocsp.digicert.com from Chrome, Mozilla Firefox, IE,» Greatis, 23 05 2015. [En línea]. Available: http://greatis.com/blog/search-redirecting-11/remove-ocsp-digicert-com.htm. [Último acceso: 27 05 2017].

[77] M. Rouse, «OCSP (Online Certificate Status Protocol),» TechTarget, [En línea]. Available: http://searchsecurity.techtarget.com/definition/OCSP. [Último acceso: 27 05 2017].

[78] C. Carter, «How Can I Remove disorderstatus.ru/order.php Virus? (Malware Removal Guide),» EasyVirusKilling, 09 07 2015. [En línea]. Available: http://easyviruskilling.com/how-can-i-remove-disorderstatus-ruorder-php-virus-malware-removal-guide/. [Último acceso: 27 05 2017].

ANEXOS

Anexo I - FORMULARIO 1/6

CARACTERIZACIÓN DEL SISTEMA (C.S.)

Nombre de la Organización / Acrónimo:

_____

Descripción general de la organización:

_____

_____

_____

_____

_____

_____

Tipo de Organización:

☐ Pública ☐ Privada ☐ Otra _____

Área o departamento donde se realizará el análisis:

_____

Nombre del/los responsable(s) del departamento / Cargo:

_____

_____

Nombre del Sistema de TI a analizar:

_____

Misión del Sistema:

_____

_____

_____

_____

Nombre del/los responsable(s) de los activos de información a quien(es) se solicita acceso para realizar el análisis y evaluación / Cargo:

_____

_____

Nombre del analizador / Cargo:

_____

Fecha del último análisis y evaluación del sistema / Nombre del informe:

_____ / _____ / _____ Informe: _____

DD MM AAAA

Fecha del análisis y evaluación del sistema a realizarse (complete este campo una vez finalizado el proceso):

_____ / _____ / _____

DD MM AAAA

Permiso de acceso a la red del Sistema de TI otorgado por la organización:

☐ Usuario ☐ Privilegiado (Recomedado) ☐ Global

Usuario: Permite conocer funcionamiento general de la red. No se permite acceso a equipos ni a modificaciones.

Privilegiado: Permite conocer funcionamiento general de la red. Se permite el acceso a los equipos para conocer su configuración. No se permite modificaciones.

Global: Permite conocer funcionamiento general de la red. Se permite el acceso a equipos para conocer su configuración. Se permite modificaciones de la red a nivel de hardware y software.

Defina el alcance que tendrá el análisis y evaluación de riesgo por departamento y por procesos (desde dónde y hasta dónde se pretende llegar con la evaluación).

_____

_____

_____

_____

_____

Defina la técnica para la recopilación de datos requeridos para el análisis y evaluación de riesgo.

☐ Entrevista ☐ Encuesta ☐ Observación

☐ Sesión de Grupo

Represente un diagrama general de red donde se dé la idea del lugar dónde se evaluará el riesgo. (Debe estar representado de la forma más general posible).

En el diagrama anterior represente con un color diferente en dónde se ubicará la herramienta para el análisis de tráfico de la red.

Defina la técnica que utilizará para realizar la captura de datos:

☐ Hub de Red ☐ Port Mirroring

☐ Modo Bridge ☐ ARP Spoofing

☐ Tap de Red ☐ Captura Remota

Nombre de la/las persona(s) dentro de la institución que brindaron apoyo en el llenado de este formulario / Cargo:

_____

_____

Anexo II - FORMULARIO 2/6

IDENTIFICACIÓN DE LA AMENAZA (I.A.)

Herramientas a utilizar en el análisis del tráfico de la red del sistema:

☐ Wireshark ☐ TCPDump ☐ Capsa

☐ Otra _____

Acción: Realizar la captura de tráfico de la red.

Fuentes de amenaza encontradas:

☐ ARP Spoofing ☐ MAC Flooding ☐ Denegación de Servicio (DoS)

☐ DHCP Spoofing ☐ VLAN Hopping ☐ Malware _____

☐ Otras _____

Evidencia(s) de la(s) amenaza(s) encontrada(s):

Nota: Cada amenaza debe tener un identificador (Id.)

Evidencia(s) de la(s) amenaza(s) encontrada(s):

Nota: Cada amenaza debe tener un identificador (Id. Amenaza).

Nombre de la/las persona(s) dentro de la institución que brindaron apoyo en el llenado de este formulario / Cargo:

_____

_____

_____

Anexo III - FORMULARIO 3/6

ANÁLISIS DE CONTROL (A.C.)

Liste los **controles técnicos implementados** en el sistema, y determine si son controles preventivos o de detección. (Controles implementados en la red del sistema que se está analizando).

Id. Control (CT#)	Controles Técnicos Implementados	Escriba "P" para controles preventivos y "D" para controles de detección.

Liste los **controles no técnicos implementados** en el sistema, y determine si son controles preventivos o de detección. (Controles implementados en la red del sistema que se está analizando).

Id. Control (CnT#)	Controles NO Técnicos Implementados	Escriba "P" para controles preventivos y "D" para controles de detección.

Liste los **controles técnicos próximos a implementarse** en el sistema, y determine si son controles preventivos o de detección. (Controles a implementarse en la red del sistema que se está analizando).

Id. Control (CTP#)	Controles Técnicos Próximos a Implementarse.	Tiempo Estimado para la Implementación (Meses).	Escriba "P" para controles preventivos y "D" para controles de detección.

Liste los **controles no técnicos próximos a implementarse** en el sistema, y determine si son controles preventivos o de detección. (Controles a implementarse en la red del sistema que se está analizando).

Id. Control (CnTP#)	Controles NO Técnicos Próximos a Implementarse.	Tiempo Estimado para la Implementación (Meses).	Escriba "P" para controles preventivos y "D" para controles de detección.

Nombre de la/las persona(s) dentro de la institución que brindaron apoyo en el llenado de este formulario / Cargo:

_____

_____

_____

Anexo IV - FORMULARIO 4/6

DETERMINACIÓN DE LA PROBABILIDAD (D.P.)

Herramientas de apoyo para a utilizar en detección de vulnerabilidades del sistema:

☐ Wireshark ☐ TCPDump ☐ Capsa

☐ Otra _____

Liste las vulnerabilidades encontradas en el sistema, y describa la fuente de obtención de cada una de ellas. (Vulnerabilidades en la red del sistema que se está analizando).

Id. Vulnerabilidad (V#)	Listado de Vulnerabilidades	Fuente de Obtención de las Vulnerabilidades

Evalúe la probabilidad de ocurrencia de cada amenaza en torno a los controles y vulnerabilidades determinadas en el sistema que se está analizando.

Alta probabilidad	**Los controles implementados son ineficaces para evitar que la vulnerabilidad sea explotada por una fuente de amenaza altamente motivada.**
Media probabilidad	Existen controles que pueden impedir que una vulnerabilidad pueda ser explotada pero la amenaza igualmente está motivada.
Baja probabilidad	La fuente de amenaza carece de motivación o capacidad, o los controles están listos para prevenir o impedir que una vulnerabilidad sea explotada.

Id. Amenaza	Amenaza	Id. Control	Id. Vulnerabilidad	Probabilidad de Ocurrencia de la Amenaza
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA

Evalúe la probabilidad de ocurrencia de cada amenaza en torno a los controles y vulnerabilidades determinadas en el sistema que se está analizando.

Id. Amenaza	Amenaza	Id. Control	Id. Vulnerabilidad	Probabilidad de Ocurrencia de la Amenaza
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA

Anexo V - FORMULARIO 5/6

ANÁLISIS DEL IMPACTO (A.I.)

Acción: Revise la "misión del sistema" en el formulario 1.

Describa de qué forma se obtendrán los datos en torno a la criticidad del sistema.

☐ Entrevista

Cargo:

_____

_____

☐ Análisis del Impacto del Negocio (BIA)

☐ Otra Documentación

Nombre de la Documentación:

_____

_____

☐ Otro

Descripción:

_____

_____

Acción: Adjunte documentación en torno a la criticidad del sistema al final de este formulario.

Describa de forma general los procesos que desarrolla el sistema de TI que se está analizando, y determine si son procesos muy críticos, críticos, o poco críticos en torno a la información de criticidad recopilada.

Id. Proceso	Descripción del Proceso	Escriba "MC" para procesos muy críticos "C" para procesos críticos "PC" para procesos poco críticos

Describa de forma general los procesos que desarrolla el sistema de TI que se está analizando, y determine si son procesos muy críticos, críticos, o poco críticos en torno a la información de criticidad recopilada.

Id. Proceso	Descripción del Proceso	Escriba "MC" para procesos muy críticos "C" para procesos críticos "PC" para procesos poco críticos

Evalúe el impacto que se tendría en cada proceso del sistema de T.I. al materializarse las amenazas. El impacto total se evalúa en base a los impactos relativos del ejercicio de cada una de las amenaza por cada proceso, y en base a esto se obtiene un valor ponderado del impacto.

Alto Impacto	**Se determina un alto impacto cuando una vulnerabilidad al ser explotada resulta en la pérdida con un altísimo costo de los principales activos tangibles o recursos; puede violentar, dañar o impedir la misión, reputación o interés de una organización.**
Mediano Impacto	En el mediano impacto al explotar una vulnerabilidad, puede resultar en una pérdida costosa de activos tangibles o recursos; puede además violentar, dañar o impedir la misión, reputación o interés de una organización pero no al nivel de un alto impacto.
Bajo Impacto	Se denomina como bajo impacto si al explotar una vulnerabilidad resulta en la pérdida de bajo costo de algunos activos o recursos tangibles, o puede afectar notablemente de una organización misión, la reputación, o interés.

Id. Proceso	Id. Amenaza	Proceso	Impacto
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO

Evalúe el impacto que se tendría en cada proceso del sistema de T.I. al materializarse las amenazas. El impacto total se evalúa en base a los impactos relativos del ejercicio de cada una de las amenaza por cada proceso, y en base a esto se obtiene un valor ponderado del impacto.

Id. Proceso	Id. Amenaza	Proceso	Impacto
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO

Anexo VI - FORMULARIO 6/6

DETERMINACIÓN DEL RIESGO (D.R.)

Riesgo: "Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización" (Magerit 3.0).

Para lograr determinar el riesgo, se requiere conocer la probabilidad que tiene una fuente de amenaza para explotar una vulnerabilidad, así como también el impacto que se tendría sobre los procesos del sistema de TI. Para lograr esto se requiere vincular en este formulario final los formularios 4 y 5 anteriores asignando valores descritos en la siguiente tabla.

Tabla de Riesgo

Impacto / Probabilidad de Amenaza	BAJO (10)	MEDIO (50)	ALTO (100)
BAJA (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10
MEDIA (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
ALTA (1.0)	Bajo 10 x 1 = 10	Medio 50 x 1 = 50	Alto 100 x 1.0 = 100

Este paso realícelo al final

Sombre los casilleros con color rojo tenue si el resultante de riesgo es de (>50 a 100), con amarillo tenue si el resultante del riesgo es (>10 a 50), y con verde tenue si el resultante es (1 a 10).

Sume el total de riesgos altos medios y bajos y complete el cuadro de recomendaciones de control para finalizar el análisis y evaluación de riesgos en el sistema de TI.

RIESGO	RECOMENDACIÓN GENERAL DE CONTROL	TOTAL DE RIESGOS (En Números)
ALTO (>50 a 100)	Si un riesgo se determina con una calificación de "Alto", se deben realizar con urgencia medidas correctivas. El sistema puede seguir operando pero un plan de acciones correctivas se debe poner en marcha lo antes posible.	
MEDIO (>10 a 50)	Si un riesgo se determina con una calificación de "Medio", se deben realizar medidas correctivas. El sistema opera con normalidad pero se requiere realizar un plan de acciones correctivas dentro de un periodo de tiempo razonable establecido por la organización.	
BAJO (1 a 10)	Si un riesgo se determina con una calificación de "Bajo", el sistema operará con normalidad y la autoridad de aprobación designada de la organización debe determinar si se requieren tomarán acciones correctivas, o decidir si se acepta el riesgo.	

En la siguiente matriz escriba de **menor a mayor** en la **segunda columna** el **valor de probabilidad** de ocurrencia de cada una de las amenazas que correspondería según la “Tabla de Riesgos” de la hoja D.R.1, y en la **primera columna** el **Id de la amenaza** que le corresponde a esa probabilidad. En la misma matriz, escriba de **menor a mayor** en la **segunda fila** el valor de **impacto** adverso que experimentaría cada uno de los procesos al materializarse las amenazas según la “Tabla de Riesgos” de la hoja D.R.1, y en la **primera fila** el **Id del proceso** que le corresponde a ese impacto.

Matriz de Riesgo del Sistema Analizado

Impacto / Probabilidad de Amenaza																		

Anexo VII - FORMULARIO 1/6

CARACTERIZACIÓN DEL SISTEMA (C.S.)

Nombre de la Organización / Acrónimo:

Dirección General de Registro Civil Identificación y Cedulación (DIGERCIC).

Descripción general de la organización:

Entidad del estado que presta servicios de identificación integral de personas y registro de hechos y actos civiles a través de medios físicos y electrónicos, garantizando calidad, seguridad, transparencia, y uso oportuno de la información, contribuyendo así a la sociedad de la información.

Tipo de Organización:

☑ Pública ☐ Privada ☐ Otra _____

Área o departamento donde se realizará el análisis:

Unidad de Gestión de Redes y Comunicaciones

Nombre del/los responsable(s) del departamento / Cargo:

Ing. Jaime Saenz – Director de Infraestructura y Operaciones

Nombre del Sistema de TI a analizar:

Magna – Sistema Principal de Cedulación

Misión del Sistema:

Sistema que presta servicios de identificación integral de personas y registro de hechos y actos civiles, enrola y emite cédulas electrónicas.

Nombre del/los responsable(s) de los activos de información a quien(es) se solicita acceso para realizar el análisis y evaluación / Cargo:

Ing. Manuel Rodríguez – Coordinador General de TIC

Ing. Jaime Saenz – Director de Infraestructura y Operaciones

Nombre del analizador / Cargo:

Andrés Reinoso Córdova – Tesista de la E.P.N.

Fecha del último análisis y evaluación del sistema / Nombre del informe:

--------- / ----------/ ---------- Informe: No existen análisis previos del sistema

DD MM AAAA

Fecha del análisis y evaluación del sistema a realizarse (complete este campo una vez finalizado el proceso):

__22__ / _05_ / __2017_

DD MM AAAA

Permiso de acceso a la red del Sistema de TI otorgado por la organización:

☐ Usuario ☑ Privilegiado (Recomedado) ☐ Global

Usuario: Permite conocer funcionamiento general de la red. No se permite acceso a equipos ni a modificaciones.

Privilegiado: Permite conocer funcionamiento general de la red. Se permite el acceso a los equipos para conocer su configuración. No se permite modificaciones.

Global: Permite conocer funcionamiento general de la red. Se permite el acceso a equipos para conocer su configuración. Se permite modificaciones de la red a nivel de hardware o software.

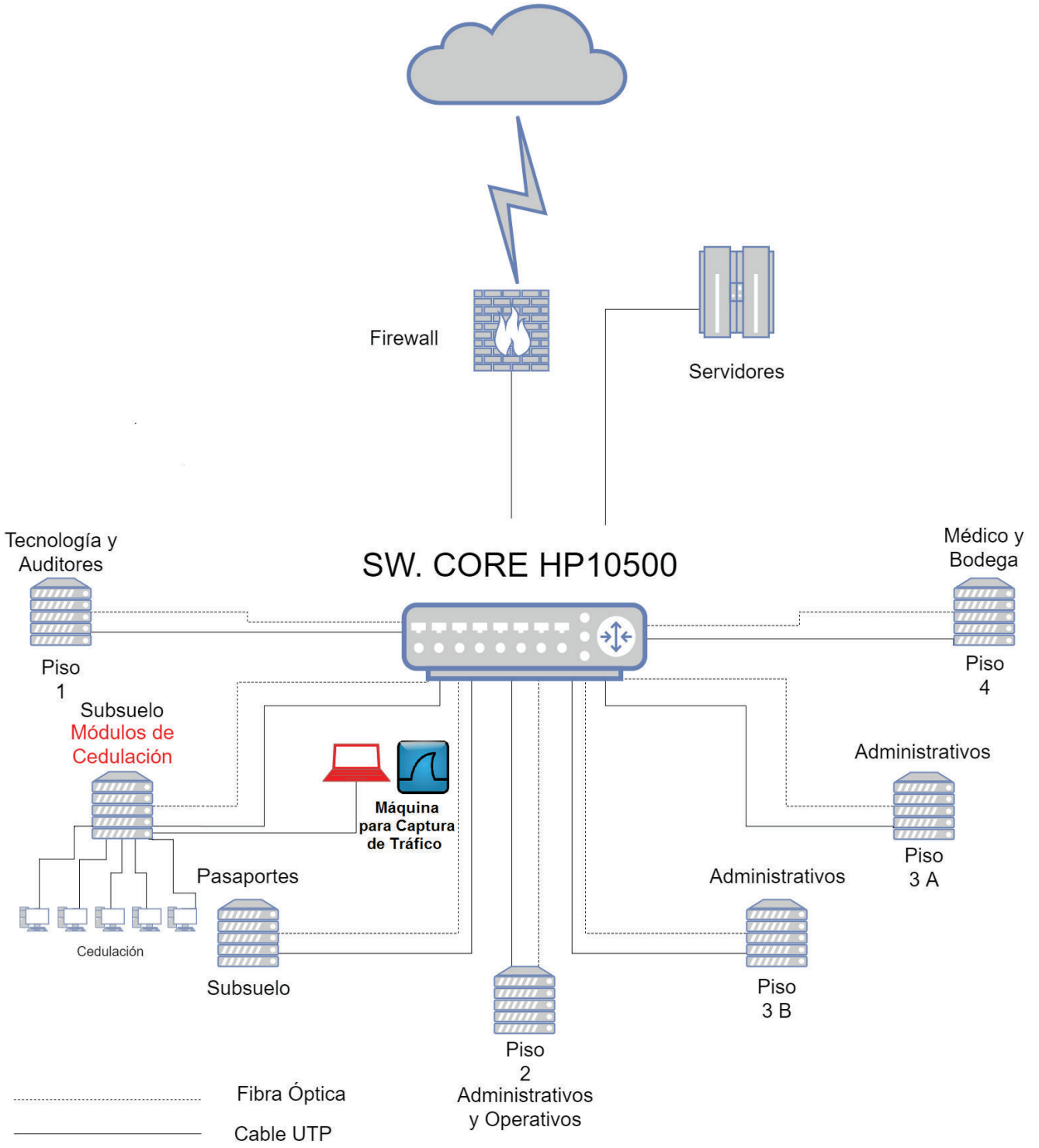
Defina el alcance que tendrá el análisis y evaluación de riesgo por departamento y por procesos (desde dónde y hasta dónde se pretende llegar con la evaluación).

Se realizará el análisis y evaluación de riesgo del Sistema Magna de TI en la LAN del sistema de cedulación mediante el análisis del tráfico de la red. Este análisis se realizará en la Matriz del Registro Civil al norte de Quito en base a las amenazas y vulnerabilidades existentes en la red local. El análisis incluirá la aplicación de los 6 formularios propuestos con lo cual se obtendrá la categorización del riesgo por procesos del sistema, se concluirá con una recomendación general dirigida a la organización para que puedan planificar un plan de tratamiento del riesgo en un plazo determinado por la institución.

Defina la técnica para la recopilación de datos requeridos para el análisis y evaluación de riesgo.

☑ Entrevista ☐ Encuesta ☑ Observación ☑ Sesión de Grupo

Represente un diagrama general de red donde se dé la idea del lugar dónde se evaluará el riesgo. (Debe estar representado de la forma más general posible).



En el diagrama anterior represente con un color diferente en dónde se ubicará la herramienta para el análisis de tráfico de la red.

Defina la técnica que utilizará para realizar la captura de datos:

☐ Hub de Red	☑ Port Mirroring
☐ Modo Bridge	☐ ARP Spoofing
☐ Tap de Red	☐ Captura Remota

Nombre de la/las persona(s) dentro de la institución que brindaron apoyo en el llenado de este formulario / Cargo:

Ing. Mauricio Correa - Analista de Gobierno de TI.

Ing. Fernando Daqui – Analista de Redes.

Anexo VIII - FORMULARIO 2/6

IDENTIFICACIÓN DE LA AMENAZA (I.A.)

Herramientas a utilizar en el análisis del tráfico de la red del sistema: Herramientas a utilizar en el análisis del tráfico de la red:

☑ Wireshark ☐ TCPDump ☐ Capsa

☑ Otra VirusTotal.com, Cain y Abel

Acción: Realizar la captura de tráfico de la red.

☐ ARP Spoofing ☐ MAC Flooding ☐ Denegación de Servicio (DoS)

☐ DHCP Spoofing ☐ VLAN Hopping ☐ Malware

1. "ldr.php" de "hzmksreiuojy.in"
2. Software malicioso de "ocsp.digicert.com", "ocsp.entrust.net", "ocsp.comodoca.com"
3. "order.php" de "disorderstatus.ru"

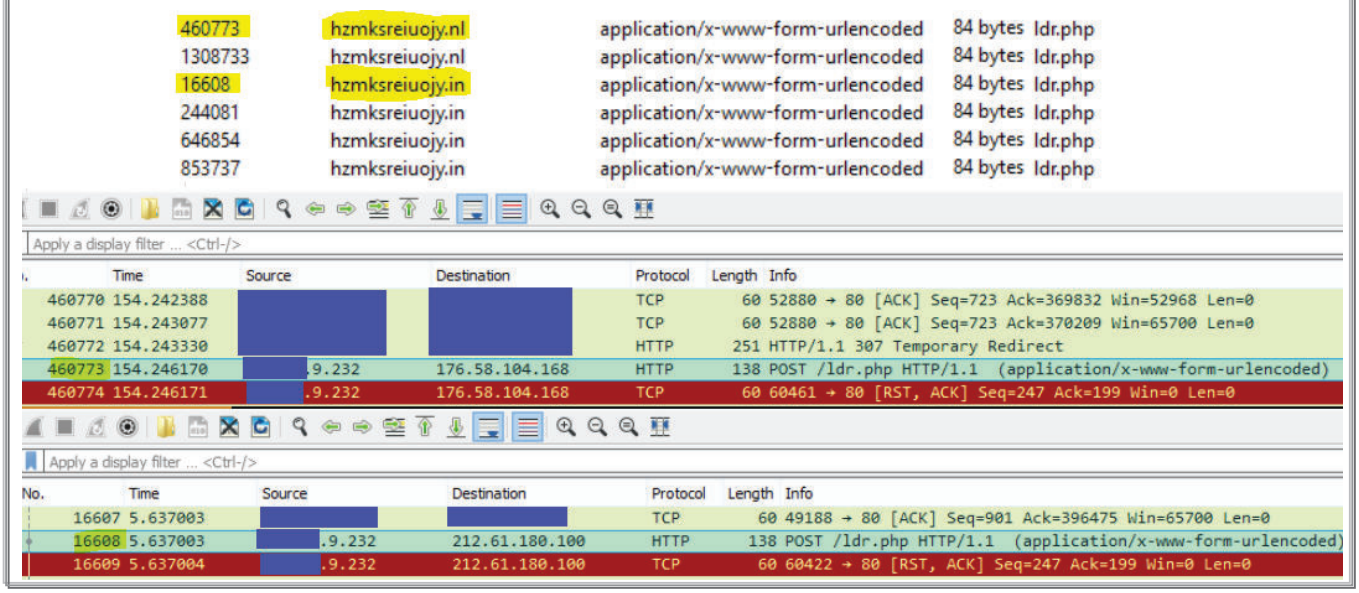
☐ Otras

Intento de conexión de páginas atacantes

Evidencia(s) de la(s) amenaza(s) encontrada(s):

Nota: Cada amenaza debe tener un identificador (Id.)

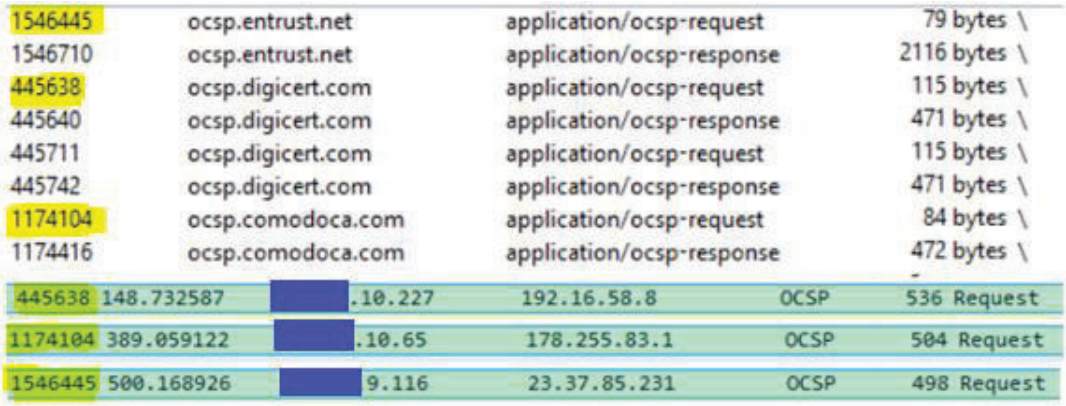
A1. Malware "ldr.php" de página "hzmksreiuojy.in" y página "hzmksreiuojy.nl"



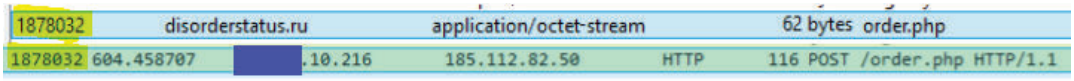
Evidencia(s) de la(s) amenaza(s) encontrada(s):

Nota: Cada amenaza debe tener un identificador (Id. Amenaza).

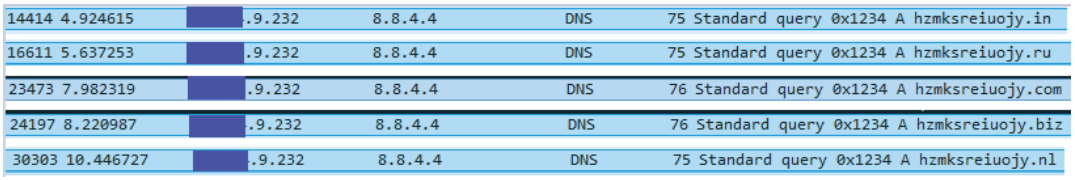
A2. Tráfico sospechoso de páginas “ocsp.digicert.com”, “ocsp.entrust.net”, “ocsp.comodoca.com”



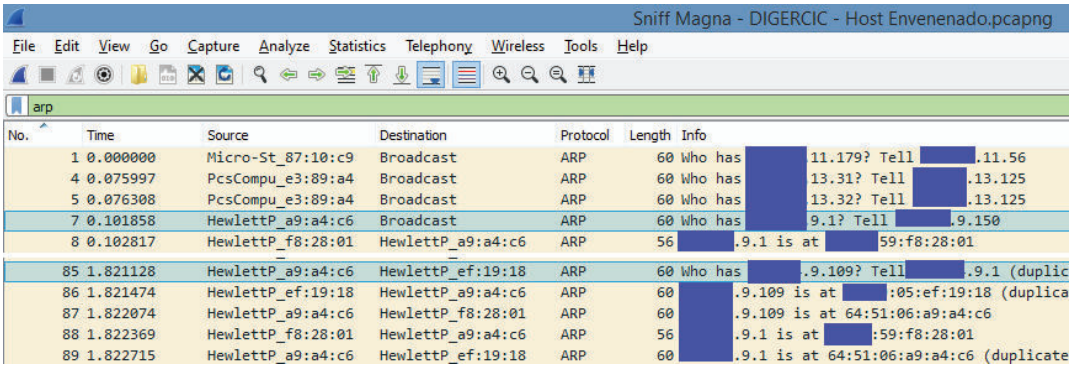
A3. Malware “order.php” de página “disorderstatus.ru”



A4. Intento de de conexión de páginas atacantes



A5. ARP Spoofing (Ataque simulado)



Nombre de la/las persona(s) dentro de la institución que brindaron apoyo en el llenado de este formulario / Cargo:

Ing. Mauricio Correa - Analista de Gobierno de TI.

Ing. Fernando Daqui – Analista de Redes.

Anexo IX - FORMULARIO 3/6

ANÁLISIS DE CONTROL (A.C.)

Liste los **controles técnicos implementados** en el sistema, y determine si son controles preventivos o de detección. (Controles implementados en la red del sistema que se está analizando).

Id. Control (CT#)	Controles Técnicos Implementados	Escriba "P" para controles preventivos y "D" para controles de detección.
CT1	Kaspersky (Antivirus para estaciones de trabajo)	D
CT2	Segmentación por VLANs	P
CT3	Anti-Spam (Magic-Spam)	P
CT4	Direccionamiento IP estático	P
CT5	Active Directory Separado (para Magna)	P
CT6	Supresión de Broadcast	P
CT7	Control por Mac Address	P
CT8	Identificación por credenciales de usuario para ingreso al sistema	P
CT9	Identificación por credenciales de usuario para ingreso a la Base de Datos	P
CT10	Servidores DNS alternos bloqueados	P
CT11	Firewall (Check Point 2400) Threat Prevention - Anti-Bot, Anti-Virus, IPS, VPN, URL Filter	P
CT12	Firewall (Check Point 2400) Threat Prevention - Anti-Bot, Anti-Virus, IPS, VPN, URL Filter	D

Liste los **controles no técnicos implementados** en el sistema, y determine si son controles preventivos o de detección. (Controles implementados en la red del sistema que se está analizando).

Id. Control (CnT#)	Controles NO Técnicos Implementados	Escriba "P" para controles preventivos y "D" para controles de detección.
CnT1	EGSI (Esquema Gubernamental de Seguridad de la Información) basado en la ISO 27002 "Código de práctica para la Gestión de seguridad de la Información" Esquema desarrollado por la SNAP (Secretaría Nacional de Administración Pública) **OBJETIVO:** Instrumento de vital importancia para todos los actores del Plan Nacional: ciudadanos, servidores, empresas, gobierno, y otros actores del estado con el fin de garantizar seguridad y confianza en el manejo de datos. Hace parte del "Plan Estratégico de Seguridad y protección de Datos".	P
CnT2	EGSI (Esquema Gubernamental de Seguridad de la Información) basado en la ISO 27002 "Código de práctica para la Gestión de seguridad de la Información" Esquema desarrollado por la SNAP (Secretaría Nacional de Administración Pública)	D
CnT3	Política de Seguridad de la Información Institucional "POL-ICM-SEI-002" **OBJETIVO**: Normar, estandarizar, controlar y asegurar la seguridad de la información institucional, en todo su ciclo de vida, mediante la implementación de medidas de seguridad preventivas, de respuesta, y de recuperación, que contribuyen a garantizar la confidencialidad. Integridad y disponibilidad de la información, en cualquiera de sus formas y medio de almacenamiento asegurando el cumplimiento de los objetivos institucionales	P
CnT4	Política de Seguridad de la Información Institucional "POL-ICM-SEI-001" **OBJETIVOS:** Generación, recuperación y conservación de respaldos – INS-GTI-IOT-001-001 Parámetros de Monitoreo de Infraestructura de TI – DCG-GTI-IOT-001-001	D
CnT5	Gestión de capacidad y Disponibilidad de Infraestructura de TI "PRO-GTI-IOT-001" **OBJETIVOS:** Generación, recuperación y conservación de respaldos – INS-GTI-IOT-001-001 Parámetros de Monitoreo de Infraestructura de TI – DCG-GTI-IOT-001-001	P
CnT6	Auditoría de Sistemas y BDD	D

Liste los **controles técnicos próximos a implementarse** en el sistema, y determine si son controles preventivos o de detección. (Controles a implementarse en la red del sistema que se está analizando).

Id. Control (CTP#)	Controles Técnicos Próximos a Implementarse.	Tiempo Estimado para la Implementación (Meses).	Escriba "P" para controles preventivos y "D" para controles de detección.
CTP1	Gestor de usuarios para monitoreo de acciones	12	D
CTP2	Interfaces VLAN directo al Firewall (Check Point 2400) Threat Prevention - Anti-Bot, Anti-Virus, IPS, VPN, URL Filter	1	P
CTP3	Interfaces VLAN directo al Firewall (Check Point 2400) Threat Prevention - Anti-Bot, Anti-Virus, IPS, VPN, URL Filter	1	D
CTP4	Parches para el S.O. contra el malware WannaCry	2	P

Liste los **controles no técnicos próximos a implementarse** en el sistema, y determine si son controles preventivos o de detección. (Controles a implementarse en la red del sistema que se está analizando).

Id. Control (CnTP#)	Controles NO Técnicos Próximos a Implementarse.	Tiempo Estimado para la Implementación (Meses).	Escriba "P" para controles preventivos y "D" para controles de detección.
CnTP1	Política para el acceso y uso de la internet y sus aplicaciones	1	P
CnTP2	ISO 27002 – Más parámetros implementados, no solo la EGSI sino abarcar más controles de ISO 27002.	12	P
CnTP3	ISO 27002 – Más parámetros implementados, no solo la EGSI sino abarcar más controles de ISO 27002.	12	D
CnTP4	Análisis y Recomendaciones del Ransomware Wannacry	0.5	P
CnTP5	Análisis y Recomendaciones del Ransomware Wannacry	0.5	D
CnTP6	Mejorar Auditoría por fases – para generar alta disponibilidad BDD de Magna	4 (Para la primera Fase)	P

Nombre de la/las persona(s) dentro de la institución que brindaron apoyo en el llenado de este formulario / Cargo:

Ing. Mauricio Correa - Analista de Gobierno de TI.

Ing. Fernando Daqui - Analista de Redes.

Ing. Hemerson Paucar - Líder de Unidad de Plataforma de Software

Anexo X - FORMULARIO 4/6

DETERMINACIÓN DE LA PROBABILIDAD (D.P.)

Herramientas de apoyo a utilizar para la detección de vulnerabilidades en la red del sistema:

☑ Wireshark ☐ TCPDump ☐ Capsa

☑ Otra _Cain y Abel, Nmap___

Liste las vulnerabilidades encontradas en el sistema, y describa la fuente de obtención de cada una de ellas. (Vulnerabilidades en la red del sistema que se está analizando).

Id. Vulnerabilidad (V#)	Listado de Vulnerabilidades	Fuente de Obtención de las Vulnerabilidades
V1	RESTRINGIDO	Análisis Interno realizado por "Líder de Unidad de Plataforma de Software"
V2	RESTRINGIDO	Análisis Interno realizado por "Líder de Unidad de Plataforma de Software"
V3	RESTRINGIDO	Análisis Interno realizado por "Líder de Unidad de Plataforma de Software"
V4	RESTRINGIDO	Análisis Interno realizado por "Analista de Redes"
V5	RESTRINGIDO	Análisis Interno realizado por "Analista de Redes"
V6	RESTRINGIDO	Análisis Interno realizado por "Analista de Gobierno de TI"
V7	RESTRINGIDO	Análisis Interno realizado por "Analista de Redes"
V8	RESTRINGIDO	Análisis Interno realizado por "Analista de Redes"
V9	RESTRINGIDO	Análisis realizado por "Evaluador de Riesgos"
V10	RESTRINGIDO	Análisis realizado por "Evaluador de Riesgos"
V11	RESTRINGIDO	Análisis Interno realizado por "Analista de Redes" y por "Evaluador de Riesgos"
V12	RESTRINGIDO	Análisis realizado por "Evaluador de Riesgos"
V13	RESTRINGIDO	Análisis realizado por "Evaluador de Riesgos"
V14	RESTRINGIDO	Reporte de usuarios del sistema

Evalúe la probabilidad de ocurrencia de cada amenaza en torno a los controles y vulnerabilidades determinadas en el sistema que se está analizando.

Alta probabilidad	**Los controles implementados son ineficaces para evitar que la vulnerabilidad sea explotada por una fuente de amenaza altamente motivada.**
Media probabilidad	Existen controles que pueden impedir que una vulnerabilidad pueda ser explotada pero la amenaza igualmente está motivada.
Baja probabilidad	La fuente de amenaza carece de motivación o capacidad, o los controles están listos para prevenir o impedir que una vulnerabilidad sea explotada.

Id. Amenaza	Amenaza	Id. Control	Id. Vulnerabilidad	Probabilidad de Ocurrencia de la Amenaza
A1	Malware “ldr.php” de página “hzmksreiuojy.in” y página “hzmksreiuojy.nl”	CT1, CT2, CT3, CT6, CT11, CT12, CnT1, CnT6, CTP2, CTP3, CnTP1	V4, V5, V6, V9, V10, V11, V12, V14	☐ ALTA ☑ MEDIA ☐ BAJA
A2	Tráfico sospechoso de páginas “ocsp.digicert.com”, “ocsp.entrust.net”, “ocsp.comodoca.com”	CT1, CT2, CT3, CT6, CT11, CT12, CnT1, CnT6, CTP2, CTP3, CnTP1, CnTP2	V4, V5, V6, V8, V9, V10, V11, V12	☐ ALTA ☐ MEDIA ☑ BAJA
A3	Malware “order.php” de página “disorderstatus.ru”	CT1, CT2, CT3, CT6, CT11, CT12 CnT1, CnT6, CTP2, CTP3, CnTP1	V4, V5, V6, V9, V10, V11, V12, V14	☐ ALTA ☑ MEDIA ☐ BAJA
A4	Intento de páginas atacantes en host local para establecer conexión a internet	CT1, CT2, CT3, CT10, CnT2, CnT6, CTP2, CTP3, CnTP1, CnTP2	V4, V5, V6, V9, V10, V11, V12, V14	☐ ALTA ☐ MEDIA ☑ BAJA

Evalúe la probabilidad de ocurrencia de cada amenaza en torno a los controles y vulnerabilidades determinadas en el sistema que se está analizando.

Id. Amenaza	Amenaza	Id. Control	Id. Vulnerabilidad	Probabilidad de Ocurrencia de la Amenaza
A5	ARP Spoofing (Ataque simulado)	CT2, CT4, CT5, CT7, CnT1, CnT3, CnT5, CTP1	V1, V2, V4, V6, V7, V8, V9, V10, V12, V13,	☑ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA
				☐ ALTA ☐ MEDIA ☐ BAJA ☐ MEDIA ☐ BAJA

Nombre de la/las persona(s) dentro de la institución que brindaron apoyo en el llenado de este formulario / Cargo:

Ing. Mauricio Correa - Analista de Gobierno de TI.

Ing. Fernando Daqui - Analista de Redes.

Ing. Hemerson Paucar - Líder de Unidad de Plataforma de Software

Anexo XI - FORMULARIO 5/6

ANÁLISIS DEL IMPACTO (A.I.)

Acción: Revise la "misión del sistema" en el formulario 1.

Describa de qué forma se obtendrán los datos en torno a la criticidad del sistema.

☑ Entrevista

Cargo:
Mauricio Correa – Analista de Gobierno de TI

Luis Sanmartín – Analista de Plataformas de Software

☐ Análisis del Impacto del Negocio (BIA)

☑ Otra Documentación

Nombre de la Documentación:
Diagrama de Estados de Magna - Application State Machine

☑ Otro

Descripción:
No existe documentación de criticidad del sistema

Acción: Adjunte documentación en torno a la criticidad del sistema al final de este formulario.

Describa de forma general los procesos que desarrolla el sistema de TI que se está analizando, y determine si son procesos muy críticos, críticos, o poco críticos en torno a la información de criticidad recopilada.

Id. Proceso (P#)	Descripción del Proceso	Escriba "MC" para procesos muy críticos "C" para procesos críticos "PC" para procesos poco críticos
P1	Estado 100 – (Estación de Captura) Sistema captura fotografía	MC
P2	Estado 120 – (Recaptura) Sistema recaptura fotografía	MC
P3	Estado 200 – (Registro en BDD Principal) Sistema registra datos en BDD	MC
P4	Estado 210 – (Validación por Abogado) Sistema redirecciona hacia abogado para validación (para extranjeros que se registran la primera vez).	C
P5	Estado 212 – (Validación Offline) Sistema registra validación offline.	PC
P6	Estado 222 – (Redirección para Investigación) Sistema registra falla en el proceso y redirecciona.	PC

Describa de forma general los procesos que desarrolla el sistema de TI que se está analizando, y determine si son procesos muy críticos, críticos, o poco críticos en torno a la información de criticidad recopilada.

Id. Proceso (P#)	Descripción del Proceso	Escriba "MC" para procesos muy críticos "C" para procesos críticos "PC" para procesos poco críticos
P7	Estado 223 – (Registro de Investigación) Sistema registra el porqué de la falla	PC
P8	Estado 224 – (Impresión de Investigación) Sistema imprime informe de la falla	PC
P9	Estado 230 – (Esperando confirmaciones, ejecución de AFIS) Sistema redirecciona a AFIS –Sistema de validación de huellas.	MC
P10	Estado 235 – (Aprobación de la Aplicación) Sistema valida criterios para aceptación	MC
P11	Estado 240 – Registro Rechazado Sistema registra rechazo.	PC
P12	Estado 245 – (Registro de terminación sin Impresión) Sistema registra finalización de proceso sin impresión	C
P13	Estado 247 - (IPI – Implementación de Seguridad a Fotografía) Sistema redirecciona a IPI –Sistema de validación de huellas.	MC
P14	Estado 250 – (Solicitud de Impresión) Sistema envía solicitud de impresión.	MC
P15	Estado 300 – (Impresión) Sistema imprime C.I.	MC
P16	Estado 340 – (Registro de Impresión) Sistema registra impresión.	C
P17	Estado 820 – Registro de Certificado Sistema registra certificado.	MC
P18	Estado 830 – Impresión de Certificado Sistema registra impresión de certificado.	MC

Evalúe el impacto que se tendría en cada proceso del sistema de T.I. al materializarse las amenazas. El impacto total se evalúa en base a los impactos relativos del ejercicio de cada una de las amenaza por cada proceso, y en base a esto se obtiene un valor ponderado del impacto.

Alto Impacto	**Se determina un alto impacto cuando una vulnerabilidad al ser explotada resulta en la pérdida con un altísimo costo de los principales activos tangibles o recursos; puede violentar, dañar o impedir la misión, reputación o interés de una organización.**
Mediano Impacto	En el mediano impacto al explotar una vulnerabilidad, puede resultar en una pérdida costosa de activos tangibles o recursos; puede además violentar, dañar o impedir la misión, reputación o interés de una organización pero no al nivel de un alto impacto.
Bajo Impacto	Se denomina como bajo impacto si al explotar una vulnerabilidad resulta en la pérdida de bajo costo de algunos activos o recursos tangibles, o puede afectar notablemente de una organización misión, la reputación, o interés.

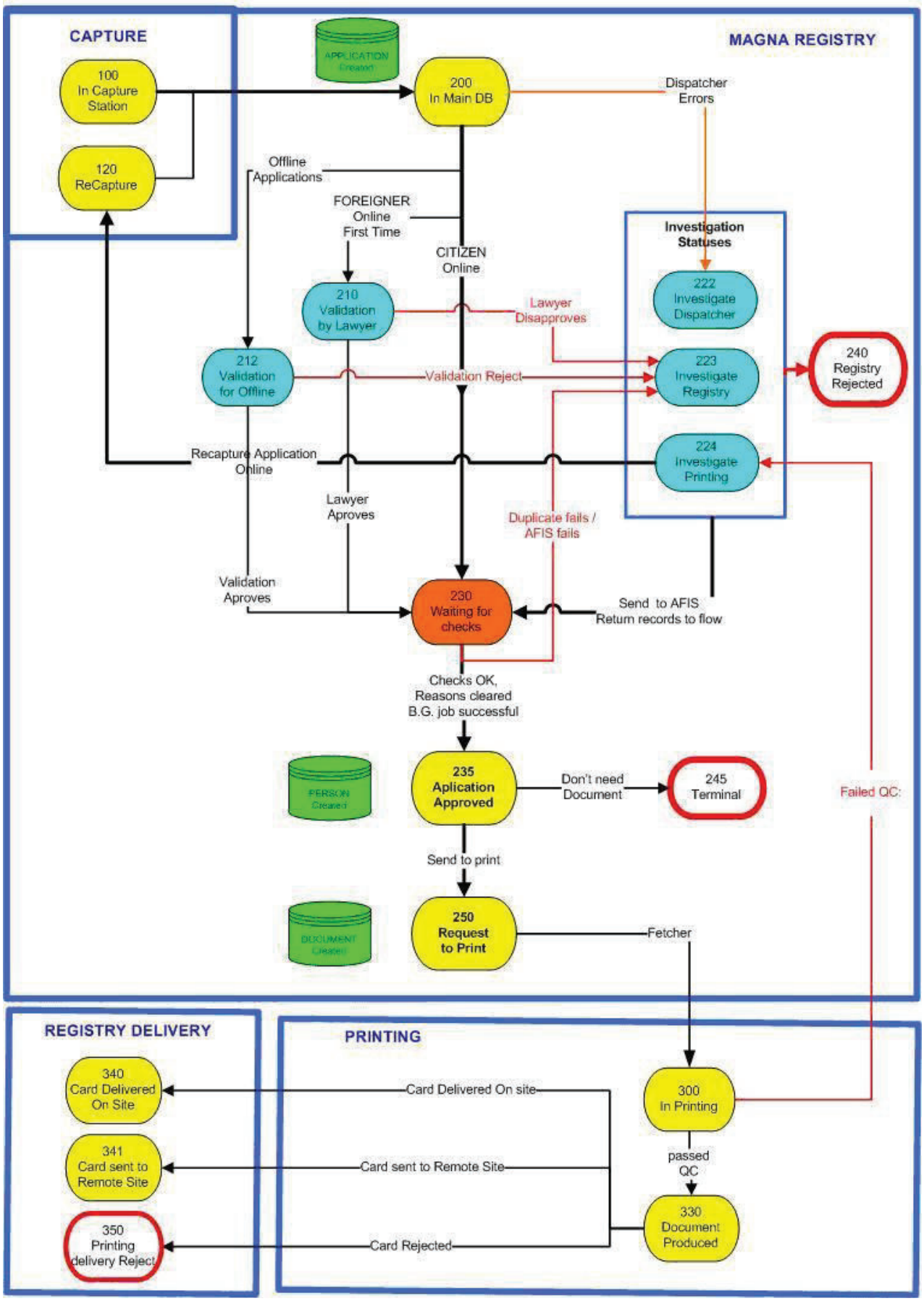
Id. Proceso	Id. Amenaza	Proceso	Impacto
P1	A1, A2, A3, A4, A5	Estado 100 – (Estación de Captura)	☐ ALTO ☑ MEDIO ☐ BAJO
P2	A1, A2, A3, A4, A5	Estado 120 – (Recaptura)	☐ ALTO ☐ MEDIO ☑ BAJO
P3	A1, A2, A3, A4, A5	Estado 200 – (Registro en BDD Principal)	☐ ALTO ☑ MEDIO ☐ BAJO
P4	A1, A2, A3, A4, A5	Estado 210 – (Validación por Abogado) Para extranjeros que se registran la primera vez	☐ ALTO ☐ MEDIO ☑ BAJO
P5	A1, A2, A3, A4, A5	Estado 212 – (Validación Offline) Para aplicaciones offline	☐ ALTO ☐ MEDIO ☑ BAJO
P6	A1, A2, A3, A4, A5	Estado 222 – (Redirección para Investigación)	☐ ALTO ☐ MEDIO ☑ BAJO
P7	A1, A2, A3, A4, A5	Estado 223 – (Investigación de Registro)	☐ ALTO ☐ MEDIO ☑ BAJO
P8	A1, A2, A3, A4, A5	Estado 224 – (Investigación de Impresión)	☐ ALTO ☐ MEDIO ☑ BAJO
P9	A1, A2, A3, A4, A5	Estado 230 – (Esperando confirmaciones, ejecución de AFIS) AFIS –Sistema de validación de huellas.	☑ ALTO ☐ MEDIO ☐ BAJO

Evalúe el impacto que se tendría en cada proceso del sistema de T.I. al materializarse las amenazas. El impacto total se evalúa en base a los impactos relativos del ejercicio de cada una de las amenaza por cada proceso, y en base a esto se obtiene un valor ponderado del impacto.

Id. Proceso	Id. Amenaza	Proceso	Impacto
P10	A1, A2, A3, A4, A5	Estado 235 – (Aprobación de la Aplicación)	☐ ALTO ☑ MEDIO ☐ BAJO
P11	A1, A2, A3, A4, A5	Estado 240 – Registro Rechazado	☐ ALTO ☐ MEDIO ☑ BAJO
P12	A1, A2, A3, A4, A5	Estado 245 – (Registro de Terminación sin Impresión)	☐ ALTO ☐ MEDIO ☑ BAJO
P13	A1, A2, A3, A4, A5	Estado 247 - (IPI – Implementación de Seguridad a Fotografía)	☑ ALTO ☐ MEDIO ☐ BAJO
P14	A1, A2, A3, A4, A5	Estado 250 – (Solicitud de Impresión)	☐ ALTO ☑ MEDIO ☐ BAJO
P15	A1, A2, A3, A4, A5	Estado 300 – (Impresión)	☐ ALTO ☑ MEDIO ☐ BAJO
P16	A1, A2, A3, A4, A5	Estado 340 – (Registro de Impresión)	☐ ALTO ☑ MEDIO ☐ BAJO
P17	A1, A2, A3, A4, A5	Estado 820 – (Registro de Certificado)	☐ ALTO ☑ MEDIO ☐ BAJO
P18	A1, A2, A3, A4, A5	Estado 830 – (Registro de Impresión de Certificado)	☐ ALTO ☐ MEDIO ☑ BAJO
			☐ ALTO ☐ MEDIO ☐ BAJO

Documentación adjunta para determinar criticidad de procesos del sistema.

ECUID – APPLICATION STATE MACHINE



Anexo XII - FORMULARIO 6/6

DETERMINACIÓN DEL RIESGO (D.R.)

Riesgo: "Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización" (Magerit 3.0).

Para lograr determinar el riesgo, se requiere conocer la probabilidad que tiene una fuente de amenaza para explotar una vulnerabilidad, así como también el impacto que se tendría sobre los procesos del sistema de TI. Para lograr esto se requiere vincular en este formulario final los formularios 4 y 5 anteriores asignando valores descritos en la siguiente tabla.

Tabla de Riesgo

Impacto / Probabilidad de Amenaza	BAJO (10)	MEDIO (50)	ALTO (100)
BAJA (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10
MEDIA (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
ALTA (1.0)	Bajo 10 x 1 = 10	Medio 50 x 1 = 50	Alto 100 x 1.0 = 100

Este paso realícelo al final

Sombre los casilleros con color rojo tenue si el resultante de riesgo es de (>50 a 100), con amarillo tenue si el resultante del riesgo es (>10 a 50), y con verde tenue si el resultante es (1 a 10).

Sume el total de riesgos altos medios y bajos y complete el cuadro de recomendaciones de control para finalizar el análisis y evaluación de riesgos en el sistema de TI.

Acciones necesarias a seguir por cada riesgo

RIESGO	RECOMENDACIÓN GENERAL DE CONTROL	TOTAL DE RIESGOS (En Números)
ALTO (>50 a 100)	Si un riesgo se determina con una calificación de "Alto", se deben realizar con urgencia medidas correctivas. El sistema puede seguir operando pero un plan de acciones correctivas se debe poner en marcha lo antes posible.	**2**
MEDIO (>10 a 50)	Si un riesgo se determina con una calificación de "Medio", se deben realizar medidas correctivas. El sistema opera con normalidad pero se requiere realizar un plan de acciones correctivas dentro de un periodo de tiempo razonable establecido por la organización.	**25**
BAJO (1 a 10)	Si un riesgo se determina con una calificación de "Bajo", el sistema operará con normalidad y la autoridad de aprobación designada de la organización debe determinar si se requieren tomarán acciones correctivas, o decidir si se acepta el riesgo.	**63**

En la siguiente matriz escriba de **menor a mayor** en la **segunda columna** el **valor de probabilidad** de ocurrencia de cada una de las amenazas que correspondería según la "Tabla de Riesgos" de la hoja D.R.1, y en la **primera columna** el **Id de la amenaza** que le corresponde a esa probabilidad. En la misma matriz, escriba de **menor a mayor** en la **segunda fila** el valor de **impacto** adverso que experimentaría cada uno de los procesos al materializarse las amenazas según la "Tabla de Riesgos" de la hoja D.R.1, y en la **primera fila** el **Id del proceso** que le corresponde a ese impacto.

Matriz de Riesgo del Sistema Analizado

Impacto / Probabilidad de Amenaza		P2	P4	P5	P6	P7	P8	P11	P12	P18	P1	P3	P10	P14	P15	P166	P17	P9	P13
		10	10	10	10	10	10	10	10	10	50	50	50	50	50	50	50	100	100
A2	0,1	1	1	1	1	1	1	1	1	1	5	5	5	5	5	5	5	10	10
A4	0,1	1	1	1	1	1	1	1	1	1	5	5	5	5	5	5	5	10	10
A1	0,5	5	5	5	5	5	5	5	5	5	25	25	25	25	25	25	25	50	50
A3	0,5	5	5	5	5	5	5	5	5	5	25	25	25	25	25	25	25	50	50
A5	1	10	10	10	10	10	10	10	10	10	50	50	50	50	50	50	50	100	100