Desarrollo de un Sistema Automatizado para Detectar Causa-Raíz de Problemas de Seguridad en una Red Carrier

Aranda, A.[(1)]; Castro, P[(2)]; Montesdeoca, N. [(3)]; Reyes, G[(4)]
[(1)] Director de la Tesina, Profesor de la ESPOL
[(2)] Miembro de la Materia de Graduación previa la obtención del Título de Ingeniería en Ciencias Computacionales, Especialización Sistemas Tecnológicos.
[(3)] Miembro de la Materia de Graduación previa la obtención del Título de Ingeniería en Ciencias Computacionales, Especialización Sistemas de Información.
[(4)] Miembro de la Materia de Graduación previa la obtención del Título de Ingeniería en Ciencias Computacionales, Especialización Sistemas de Información.
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral
Campus Prosperina, Km. 30.5 vía Perimetral, Guayaquil, Ecuador
{aaranda, pcastro, nmontesdeoca, greyes}@fiec.espol.edu.ec

***Abstract*— This project demonstrates the development of a system to aid in making decisions based on event correlation based on security alerts, logs of Cisco and Linux, and other parameters. This tool has an algorithm of analysis will be based on knowledge of the topology graph of the network and the possible causes and logical operations on events that the operator so within N steps. Also, the system will work in conjunction with traffic sensors (sniffers) strategically located on the network. On the other hand the solution to detect, diagnose and report promptly the events in the network, offering essential information they need to know the network engineers in natural language showing them on a console in real time that users spend more time doing specific networks, but not in identifying problems..**

***Resumen*—El presente proyecto muestra el desarrollo de un sistema para la ayuda en la toma de decisiones en base a la correlación de eventos en base a alertas de seguridad, logs de equipamientos CISCO y Linux, y otros parámetros. Esta herramienta constará con un algoritmo de análisis que tendrá como base de conocimiento el grafo de la topología de la red y las posibles causas y las operaciones lógicas sobre eventos que el operador hiciere en N pasos. También el sistema trabajará en conjunto con sensores de tráfico (sniffers) estratégicamente ubicados en la red. Por otro lado la solución permite detectar, diagnosticar y reportar rápidamente los eventos ocurridos en la red, ofreciendo información esencial que necesitan conocer los ingenieros de redes mostrándolos en lenguaje natural en una consola en tiempo real, tal que los usuarios destinarán más tiempo a las tareas específicas de redes, mas no en la identificación de problemas.**

I. INTRODUCCION

Los proveedores de banda ancha realizan fuertes inversiones en sus redes, permitiendo a los usuarios disfrutar de actividades tales como la trasmisión continua de audio y video, juegos en línea, conferencias vía internet, adquisición y distribución de contenidos. Los abonados se basan cada vez más en estas aplicaciones como componentes de valor de la vida cotidiana. Sin embargo hay usuarios que han encontrado otras maneras de poner la red a trabajar con fines malignos.

1.1. Tráfico Malicioso en Redes

Uno de los tráficos maliciosos más frecuentes son los correos o mensajes electrónicos no deseados [3], el tráfico malicioso puede ser utilizado como herramienta para realizar ataques en las redes, también pueden tener metas específicas tales como el secuestro de los equipos de los abonados o robo de información. Este y otros tipos de ataques son la principal preocupación que enfrentan los administradores de las Tecnologías de Información IT, ya que si bien es cierto que tienen que ofrecer a sus clientes la mayor variedad de recursos y satisfacer las demandas más exigentes de manera eficiente y flexible. Esto presenta riesgos potenciales, tales como usuarios accidentalmente introduzcan virus o el uso de equipos clientes para ingresar a servidores o dispositivos críticos del ISP.

La situación antes mencionada hace que los ISP enfrente cargas financieras superiores, estas incluyen:

- El incremento del servicio de atención al cliente, ya sea este mediante llamadas o email, debido a los síntomas de una infección o ataque en la red.

- Gastos de funcionamiento para protección de la red.
- Gastos por la tarea de restauración de los servicios de red.
- Inversiones para la construcción de una arquitectura de una arquitectura segura, basada en cada una de las líneas de negocio de los usuarios.

Además de los gastos financieros antes mencionados debido al tráfico malicioso, este puede causar otro tipo de problemas tales como:

- Robo de información
- Caída de Servicios
- Infecciones Generalizadas.
- Uso indebido de recursos de la red.
- Impacto en la reputación de la empresa.

Para mitigar o evitar cada uno de los problemas expuestos, los administradores de seguridad utilizan una serie de herramientas heterogéneas en la red y aplicaciones diseñadas para garantizar puntos de seguridad selectivos basados estratégicamente en las zonas de mayor riesgo. Estas herramientas, provee diferentes tipos de información, las cuales se almacenan de diferentes formas tales como: bases de datos, registros en archivos de texto; además se presentan a través de múltiples interfaces (web, aplicaciones de escritorio y notificaciones mediante correo). Cuando ocurre un problema en la red, el administrador tiene que consultar cada una de estas herramientas y basándose en sus altos conocimientos él puede comprender y entender el evento que se suscito, topándose muchas veces con falsos positivos los cuales le costaron tiempo y recursos.
Este sistema no es óptimo debido a que el personal debe tomar varias horas del tiempo para realizar esta gestión en vez de destinar más tiempo a las tareas específicas de administración de redes.

1.2. Tráfico Malicioso en Redes

Puesto que el proveedor debe garantizar a sus clientes un ambiente donde puedan desarrollar las actividades de su negocio de forma confiable, este también debe promover el desarrollo de sistemas de administración que incluyan políticas y procesos que garanticen una arquitectura tecnológicamente segura. Esta arquitectura segura se establece en base a dos pilares fundamentales: control total y visibilidad total.

La ***visibilidad total*** comprende en la *identificación* y asignación de niveles de autorización para cada abonado. *Monitoreo* del desempeño y comportamiento de la red de manera continua. Recolección, *correlación* y análisis de eventos suscitados en la red.

El **control total** cubre la alta disponibilidad y la *fortaleza* de la infraestructura para que los eventos malintencionados no puedan afectar la red, también consiste en control activo de la información, prevención de pérdida de datos; políticas de difusión y *cumplimiento* de estas, aprovisionamiento y protección en servicios entregados al usuario manteniendo las *restricciones*.

Nuestra solución contribuirá a tener una visibilidad total y poder actuar de forma preventiva y reactiva ante anomalías de tráfico malicioso en la red. Además correlacionará y mostrará información esencial rápidamente de los problemas de tráfico malicioso mostrando su origen ofreciendo vistas predefinidas centradas en las incidencias las cuales están ocurriendo en la red. Las características de esta solución son: *recopilación* en una única base de datos con todos los eventos detectados por los diferentes sniffers colocados en la red y de la información obtenida a través de fuentes adicionales; *simulación* de los pasos que un administrador de red realizaría a través de las diferentes fuentes para saber exactamente lo que está pasando en la red, cada vez que aparezca un evento sospechoso en una de las fuentes, al hacer esta *relación* se podrá obtener más evidencias, mayor información acerca de las incidencias que el malware ocasionó en la red, y conclusiones acerca de este evento y una vez encontrado el inconveniente se indicará a cada uno de los equipos infectados, para que los administradores de los mismos tomen las medidas necesarias.

II. FUNDAMENTOS TEÓRICOS

La seguridad informática se basa en sostener tres bases importantes como la disponibilidad, confidencialidad e integridad de los activos de información de una persona o empresa, estos activos de información están en constante amenaza por personas que desean explotar vulnerabilidades a través de malware. Para el caso de un carrier /ISP su principal activo es la red de telecomunicaciones sobre la cual presta servicios.

Uno de los más comunes generadores *de trafico malicioso* es el Malware que viene del inglés (malicious software - programa malicioso), es un programa que se infiltra sin consentimiento del propietario para obtener datos o dañar el computador.

El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto; el software es considerado malware en base a las intenciones del autor a la hora de crearlo. El término malware incluye virus, gusanos, troyanos, la mayoría de los rootkits, spyware, adware intrusivo, crimeware y otros software maliciosos e indeseables, malware no es lo mismo que software defectuoso, este último contiene bugs peligrosos pero no de forma intencionada.

Estos malware traen como consecuencia retrasos en el ambiente laboral, un estrés operativo, datos irreales mostrando una mala imagen de la empresa marcándola como poco segura y poco confiable por lo que los clientes podrían preferir la competencia y con ello pérdidas monetarias.

2.1. Herramientas que generan Tráfico Malicioso

Una herramienta común que genera tráfico malicioso son los escaneo de direcciones estos se los puede definir como un rastreo de posibles víctimas donde se trata de identificar puertos abiertos cuya información nos serviría para una siguiente fase de explotación. Este tipo de rastreo tiene mayor impacto y cambiaría su nombre como ataque en el momento que consume recursos excesivos de nuestra red.

Un ***escaneo de direcciones*** puede ser ejecutado intencionalmente (en el caso de un hacker) o no intencionalmente (en el caso de un computador infectado por un virus o gusano) que inicia un gran número de nuevos flujos de paquetes de información a muchas máquinas destino en un puerto específico. Normalmente esto indica que un gusano o Botnet está tratando de encontrar e infectar otras máquinas propagándose por la red. Luego de escanear todo utiliza este informe para identificar los computadores infectados, los que serán los atacantes potenciales.[10]

Las ***Botnet*** estás se forman mediante un bot máster que busca equipos en internet que encuentre vulnerables o desprotegidos a los que puede infectar, cuando los encuentra los infectan y comunican a su creador y luego quedan oculto hasta que se le indique realizar una tarea. [4] [5]

Algunas de las tareas realizadas por los bot son: Infectar a más máquinas en la red o internet, enviar Spam, ser utilizados para realizar phishing, también como un medio de extorsión a un sitio web el cual este bajo su control, fraudes como aumentar la facturación de publicidad web al dar clic automáticamente de alguna página que pague por este servicio, también pueden ser utilizados para realizar ataques de denegación de servicios.

Estos son muy complicados de localizar, porque casi nunca son infectados por el Bot máster, más bien son infectados por computadores que anteriormente hayan sido infectados tal como se muestra en la figura 2.1, la cantidad de bot infectados puede llegar a ser miles o cientos todos bajo el control de un bot máster.

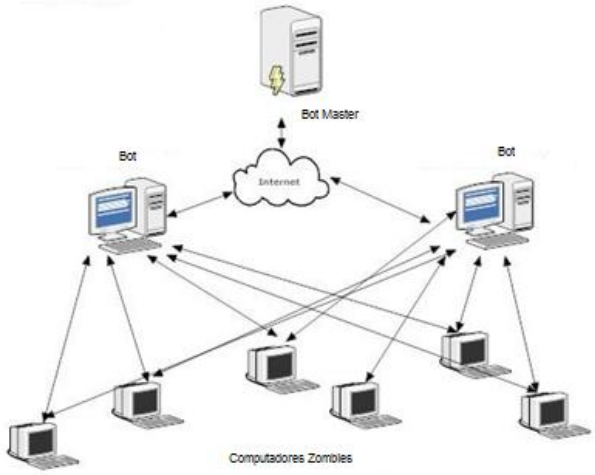

Figura 2.1 Forma de ataque de una Botnet[6]

Spam es un fenómeno que va en aumento día a día, y representa un elevado porcentaje del tráfico de correo electrónico total. Además, a medida que surgen nuevas soluciones y tecnologías más efectivas para luchar contra el spam, los spammers también desarrollan técnicas para comprometer equipos por medio de gusanos o virus para que reenvíen este tipo de correos a diferentes emails los cuales constan en su listado.

Una forma mediante la cual un spammer puede realizar el envío de estos mensajes es a través de servidores mal configurados. Estos servidores que permiten que se envíe correos a través de ellos, se los denomina Open Relay. [2]

Para solucionar esto (o castigar a la gente que tiene el MTA aceptando este puenteo de correos para cualquier lugar) se crearon listas negras en tiempo real que bloquean dichos hosts, y para que se saque una IP de estas listas, se deben pasar ciertas pruebas y esperar cierto tiempo.

A continuación enumeraremos varios ataques que se suscitan en la red los cuales son detectados por las fuentes en este proyecto.

Un DoS es un ataque a sistemas de información o redes, que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. [8]

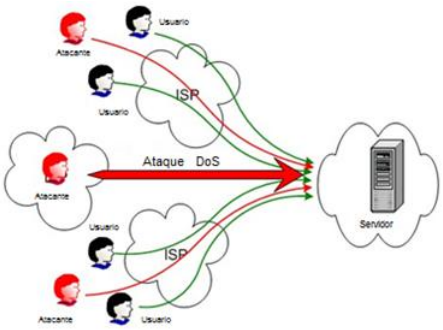

Figura 2.2 Ataque DoS [7]

El ataque se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios tal como vimos en la figura 2.2; por eso se le dice "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta técnica es usada por los llamados Crackers para dejar fuera de servicio a servidores objetivo.

Un ataque DoS puede ser perpetrado de varias formas, aunque básicamente consisten en: Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.

Luego de revisar algunos de los diferentes ataques a los que la red está expuesta podemos concluir que los ataques son un motivo muy importante por cual las empresas deben tener herramientas que permitan montar una arquitectura basada en control total y visibilidad total.

III. Recopilación de los Datos y Centralización de la Información

Actualmente existen muchas herramientas y soluciones que permiten a las empresas administrar mejor la seguridad en sus redes. Como se indico anteriormente, la solución que se plantea no trata de suplantar estas herramientas, sino que las mismas sean fuentes de alimentación para la correlación. Mientras más fuentes sean, más datos tendremos de las incidencias. Nuestro sistema recopila datos de diferentes fuentes las cuales se encuentran ubicadas estratégicamente en la red tal como se puede observar en la figura 3.1, analizando o buscando alguna anomalía en el tráfico de la red.

Para recopilar la información, se utilizará un servidor en el cual se centralizara la información el cual para términos de análisis se lo denomina SRC (Servidor Recolector Central). Sin embargo, cada fuente tiene métodos y formas de almacenamiento diferentes; por lo tanto, uno de los objetivos de esta sistema fue tomar los datos obtenidos de cada fuente, traducirlos a un solo lenguaje y enviarlo al SRC el cual consta de una base de datos mysql en donde se almacenará la información ya traducida.

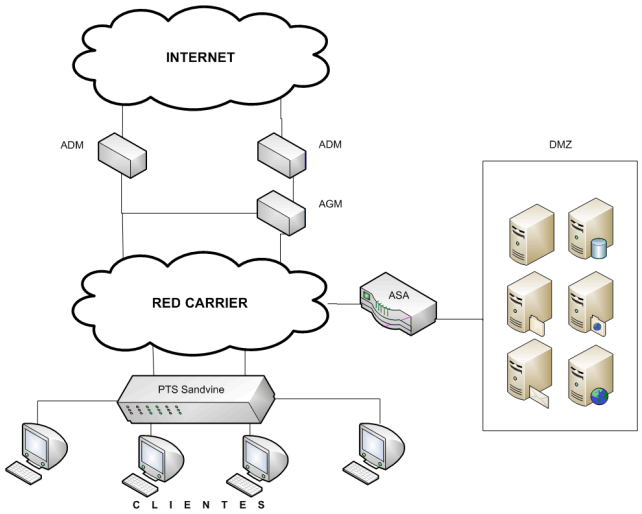

Figura 3.1 Esquema de la red

En el **Figura 3.2** se muestra las fuentes y los mecanismos que se utiliza para la extracción de los datos de de cada una de ellas y el almacenamiento en la base unificada del SRC.

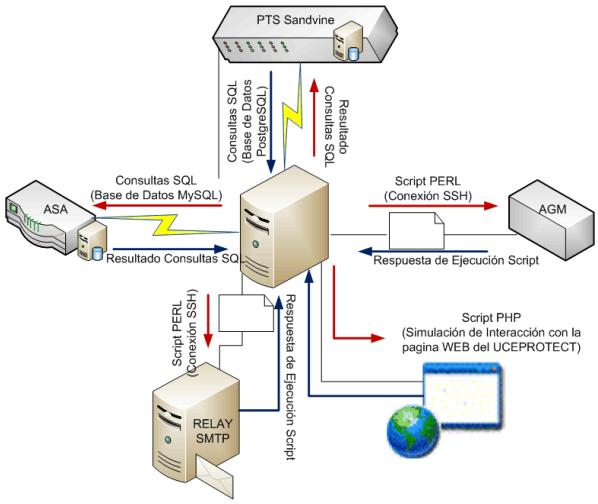

Figura 3.2 Esquema de la red

A continuación detallamos los sniffers y otras fuentes que se utilizo para esta solución:

- ***PTS Sandvine*** Sandvine es un producto de seguridad diseñado para identificar y mitigar el único conjunto de amenazas que existen en las redes de banda ancha, reconociendo los síntomas de la infección en tiempo real. [12]

Una estrategia de defensa construida sobre la política PTS para redes de cualquier tamaño y cualquier número de enlaces asimétricos, permiten a la solución a concentrarse en las tareas: Identificar y bloquear las fuentes de spam de correo electrónico saliente, prevención de la propagación de gusanos en la red, detección y bloqueo de ataques de denegación de servicio (DoS). El método utilizado para obtener los datos es un script que realiza consultas a una base postgresql ubicada en el PTS de Sandvine; los ataques obtenidos son: Address Scan, Syn Floods, Flow Floods, Spammers y User Bandwidth. Esta información es almacenada en la base de datos de SRC en la tabla llamada Sandvine, los datos obtenidos son los siguientes: ip_atacante, ip_victima, tiempo que duro el ataque, fecha detectado, el tipo de ataque y el protocolo que utiliza.

- El ***ASA*** el cual es un firewall de marca CISCO, su forma de trabajo es basado en firmas para detectar y detener ataques en la red. En base a que acción describe cada una de las firmas indicadas, podemos agruparla las actividades detectadas en la red de la siguiente manera.
  - **DDoS**: UDP Bomb, OpenSSL SSL/TLS Malformed Handshake DoS, MSSQL Resolution Service Stack Overflow, Oracle BEA WebLogic Server Apache Connector Buffer.
  - **Escaneo de Puertos:** ICMP Network Sweep w/Echo, TCP SYN Host Sweep, TCP SYN Port Sweep.
  - **Spamming:** Grum bot

Los datos de firewall se obtienen por medio de la aplicación Cisco IME, esta aplicación lo coloca en un base datos de Mysql en tablas llamas event_table, estas tablas son copiadas a nuestra base local de mysql por medio de un proceso batch que ejecuta un script en php para la copia la tabla en nuestra base local y asi ser accedida para obtener los datos que necesitamos como: ip atacante, ip victima, riesgo valorado por el ASA, la fecha de la detección, el tipo de ataque y el protocolo.

Las tarjetas ***AGM/ADM*** son módulos propios de conmutadores Catalyst 6500 Series y Cisco 7600 Series que ofrecen una solución para la defensa de los recursos en línea contra la masiva negación distribuida de servicios (DDoS). Estos dispositivos almacenan la información de los ataques que se están realizando en el momento a la red del proveedor, los mismos que están siendo mitigados por el mismo. Para conocer estos ataques el administrador de la red debería conectarse via SSH al AGM y mediante comandos propios de este dispositivo se obtiene la siguiente información: IP y puerto que está siendo atacado, IP y puerto que está realizando el ataque, cuanto tiempo dura el ataque, protocolo que utiliza, acción realizada para mitigar este ataque, fecha de inicio y fecha fin del ataque.

- ***Alertas enviadas por correos enviados por CERTs***

Correos recibidos de CERTs a nivel mundial. En estos correos se indican IPs y tipos de ataques que las mismas están realizando. Cada CERT tiene su propio formato de envío de correo los mismos contiene información de IPs que han sido encontradas como infectadas por algún tipo de malware y son reportados a una cuenta de correo especial, este cuenta de correo se encuentra en un servidor POP del la empresa destinataria del correo, y para obtener la información de los mismos se realiza una conexión vía SSH al servidor POP, el script también se encarga de filtrar solamente la información que es importante para nuestro sistema y la envía a la base de datos de SRC, para que esta información también pueda ser correlacionada con las otras fuentes descritas anteriormente según el tipo de ataque que sea detectado.

- ***Listado UCEPROTECT***

Es una página web donde se registran las IPs consideradas mayores spammers. Cada empresa puede tener uno o más ASNs (Autonomous System Number), el mismo que al ingresar en la página indicada anteriormente mostrará un listado de todas las IPs de la empresa que han sido registradas como generadoras de SPAM junto al número de ataques que se han realizado. [15]

Para la recolección de datos por medio del ASN se ejecuta un script desarrollado en javascript, el cual se conecta a varios scripts php los cuales realizan los siguientes pasos:

- Realiza la carga de todo el sitio para poder obtener el subchannel quemado en el código del sitio, el cual es necesario para enviarle cualquier petición POST.
- Luego de obtenido el subchannel, ya se puede realizar la petición POST para obtener todas las asignaciones comprometidas.
- Finalmente una vez obtenidas todas las asignaciones se procede a guardarlos en la base local.

Los datos obtenidos con este script son guardados en la tabla Uceprotect y contendrá los siguientes campos: ip, máscara y la fecha de detección.

IV. Implementación del Sistema

La implementación contempla dos componentes esenciales para su correcto funcionamiento: los scripts que se ejecutan para obtener/correlacionar la información de las diferentes fuentes y la interface del usuario que no es otra cosa que la herramienta que el usuario final utilizará para ver la información procesada por los scripts.

4.1 Scripts

En esta etapa se implementan cada uno de los scripts necesarios para el correcto funcionamiento del sistema, los mismos se encontrarán alojados en el servidor SRC y se ejecutan mediante crontab, procurando que los mismos se ejecuten en horario y frecuenta tal que no afecte al rendimiento de los equipos y que además mantenga actualizada la información de la forma más periódica posible.
Debido a la complejidad, tiempo de ejecución y función que desempeña de estos procesos, los scripts se clasifican en tres grupos:

- Scripts de Obtención de Datos de las Fuentes.
- Script de Correlación.
- Script de Identificación y envío de correo al atacante.

4.2 Interfaz de Usuario

Como su nombre lo indica, esta va a ser la herramienta con la cual el usuario va a tener interacción. La misma constará de paneles que mostrarán resúmenes en tiempo real de la situación en la red.

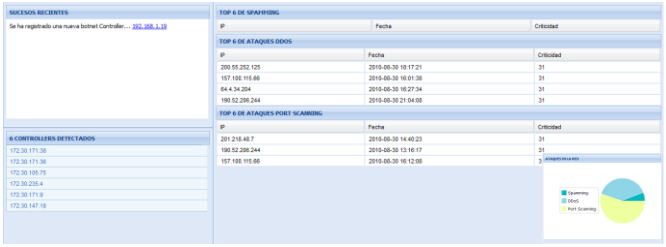

Figura 4.1 Interfaz de Usuario

Para la implementación de nuestro sistema se escogió una librería que utiliza Javascript en la cual se pueda desarrollar aplicaciones web interactivas y amigables para el usuario final ya que la herramienta debe servir de apoyo para el monitoreo, ser fácil de interpretar y agradable de usar. La herramienta escogida para implementar la interfaz de usuario es ExtJS.
Esta herramienta nos permite hacer uso de tecnologías como AJAX, DHTML y DOM, además es altamente productivo para la creación y el mantenimiento de aplicaciones web de alta calidad y permite crear efectos que hacen más agradable la aplicación. Estos efectos son parte de la experiencia que disfruta el usuario y pueden definir el punto de calidad que distingue una solución de las demás, dándole un uso correcto, puede mejorar la usabilidad de las aplicaciones.

V. Pruebas y Resultado

Nuestro sistema trata de facilitar la administración, el control y la visualización de los diferentes ataques que se realizan en nuestra red. Anteriormente se tenía una visualización parcial de los diferentes ataques que se suscitaban en la red basándose en las diferentes fuentes de detección.
Por ello presentamos en esta sección las pruebas realizadas basadas en el tiempo que un administrador o encargado de la red se tardaría en dar el seguimiento a un problema reportado midiendo la diferencia entre el tiempo tomadas el realizar un monitoreo manual y el tiempo de realizarlo por medio del sistema.

Las siguientes tablas presentan las comparaciones de tiempo entre lo que le toma al administrador de la red realizar una inspección de un posible evento en forma no automatizada versus el que toma consultarlo en el sistema. Para estas pruebas se tomaron los siguientes escenarios:

Escenario 1:

Sandvine reportó la existencia de una IP que estaba realizando un Escaneo de direcciones. El administrador realizó la correlación de la forma no automatizada, obteniendo el tiempo de respuesta mostrado en la tabla 5.1. Después ingresó a nuestro sistema para obtener la información ya correlacionada, obteniendo un tiempo de respuesta mostrado en la tabla 5.2.

PROCESO MANUAL		
1	Tiempo en conectarse al sandvine	57 seg
2	Tiempo en buscar la IP en los diferentes tipos de ataque	3 min 48 seg
3	Tiempo que tomo en conectarse al CISCO IME (ASA)	7 min 3 seg
4	Tiempo que tomo en realizar la correlación de la información obtenida.	1 min 44 seg
TOTAL TIEMPO		**13 min 58 seg**

Tabla 5.1.- Tiempos Escenario 1- Proceso Manual.

VIA SISTEMA		
1	Tiempo en conectarse al Sistema	11 seg
2	Tiempo en colocar parámetros de búsqueda en el sistema	33 seg
3	Tiempo de respuesta	17 seg
TOTAL TIEMPO		**57 seg**

Tabla 5.2.- Tiempos Escenario 1- Resultados Obtenidos por Sistema.

Escenario 2:

Se notificó en el Sandvine una IP que se encuentra enviando SPAM. El administrador realiza la tarea de correlación de forma no automatizada y luego vía sistema; los resultados obtenidos están en las tablas 5.3 y 5.4.

PROCESO MANUAL		
1	Tiempo en conectarse al sandvine	58 seg
2	Tiempo en buscar la IP en los diferentes tipos de ataque	6 min 38 seg
3	Tiempo que tomo en conectarse al CISCO IME (ASA)	26 seg
4	Tiempo que tomo en conectarse al servidor de correo de email recibidos por CERT	2 min 14 seg
5	Tiempo que tomo en realizar la correlación de la información obtenida	2 min 49 seg
TOTAL TIEMPO		**13 min 15 seg**

Tabla 5.3.- Tiempos Escenario 2- Proceso Manual.

VIA SISTEMA		
1	Tiempo en conectarse al Sistema	12 seg
2	Tiempo en colocar parámetros de búsqueda en el sistema	28 seg
3	Tiempo de respuesta	10 seg
TOTAL TIEMPO		**50 seg**

Tabla 5.4.- Tiempos Escenario 2- Resultados Obtenidos por Sistema.

Escenario 3:

El administrador realizó la búsqueda de una IP que el módulo AGM reporto que se encuentraba realizando un Ataque DDoS; realizó la correlación obteniendo el tiempo de respuesta mostrada en la tabla 5.5 y realizó la consulta vía sistemas obteniendo el tiempo mostrado en la tabla 5.6.

PROCESO MANUAL		
1	Tiempo en conectarse al Sandvine	58 seg
2	Tiempo en buscar la IP en los diferentes tipos de ataque	4 min 7 seg
3	Tiempo que tomo en conectarse al CISCO IME (ASA)	25 seg
4	Tiempo que tomo en buscar en las diferentes firmas la IP en CISCO IME (ASA)	5 min 39 seg
5	Tiempo que tomo en realizar la correlación de la información obtenida	2 min 27 seg
TOTAL TIEMPO		**11 min 9 seg**

Tabla 5.5.- Tiempos Escenario 3- Proceso Manual.

VIA SISTEMA		
1	Tiempo en conectarse al Sistema	8 seg
2	Tiempo en colocar parámetros de búsqueda en el sistema	19 seg
3	Tiempo de respuesta	18 seg
TOTAL TIEMPO		**35 seg**

Tabla 5.6.- Tiempos Escenario - Resultados Obtenidos por Sistema.

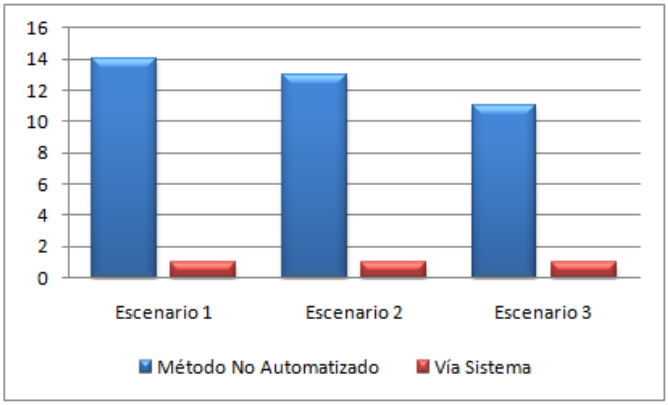

Figura 5.1 Escenario 1 comparación de tiempo.

Como podemos observar el la Figura 5.1, el tiempo que le toma al administrador en consultar la información ya correlacionada en nuestro sistemas es diez veces menor que el tiempo que le toma realizar la correlación en forma no automatizada.

Escenario 4:

Se necesitaba obtener un reporte de las botnet que han afectado nuestra red tomando como fecha inicial 4 junio 2011 hasta 6 junio de 2011 y verificar cuantos ataques realizaron y cuantas victimas tuvieron en ese periodo de tiempo.

Para que el administrador pudiera conocer la información anterior, tenía que ingresar a la base de datos del ASA y buscar todos los ataques Swizor; con esta acción encontraba las botnets. Después por cada botnet tenía que buscar que IPs han tenido un Escaneo de Direcciones cuyo atacante era una de las IPs encontradas en la primera búsqueda. Y para finalizar el reporte, contabilizar el número de ataques que cada una tuvo. Como se puede observar este trabajo era muy tedioso y tomaba demasiado tiempo al administrador, restando el tiempo valioso que el mismo podría estar utilizando en tareas más administrativas. Nuestro sistema ya lo realiza, para esto mostramos la tabla 5.7 donde se ve el tiempo que se toma el administrador en obtener esta información.

VI. CONCLUSIONES

Una vez concluido el Sistema Automático para Detectar Causa-Raíz de Problemas de Seguridad en una Red Carrier podemos concluir:

1. Nuestra herramienta facilita al administrador de la seguridad la correlación entre cinco diferentes fuentes de detección de malware, basándose en algoritmos que permiten optimizar la información obtenida y omitir falsos positivos, que en muchos casos han sido pérdida de tiempo y recursos para quienes han tenido que dar seguimiento a los mismos.

2. La herramienta proporciona una poderosa opción que es la detección de posibles Botnet que están afectando la red, esta opción es importante ya que detectar botnet manualmente es un trabajo muy tedioso, y reconocer los bots para notificarles tomaría mucho tiempo, esta herramienta ya lo realiza en forma automática.

3. La interface gráfica y amigable que proporciona este sistema permite mantener informado en tiempo real al administrador de la seguridad, de los diferentes ataques que se estén suscitando en la red, obtener estadísticas por intervalos de tiempos por datos generales y por datos específicos como: IP atacantes, IP víctima y tipos de ataque .

4. Un importante aporte denuestra herramienta es la notificación a clientes. Si se detecta que una IP está realizando ataques constantemente, o está formando parte de una botnet, el sistema reconoce a que cliente pertenece la IP y notifica para que tome las medidas pertinentes según sea el caso.

5. En base a los resultados de las pruebas podemos comprobar una enorme brecha en tiempos entre los que demoraba un usuario en realizar una inspección manual y el tiempo que se toma en el sistema monitorear la misma incidencia; con esto podemos concluir que nuestro sistema: reduce los tiempos de inspección y nos permite tener una visibilidad total de la red en tiempo real.

6. Se puede aumentar la visibilidad y el control de la seguridad de la red aumentando fuentes de detección heterogéneas.

VII. RECOMENDACIONES

Las recomendaciones relevantes que se puede realizar en este proyecto de graduación son:

1. Se podría aumentar tipos ataques que se suscitan en la red basando en un estudio más profundo de cada uno de las fuentes de detección.

2. Como segunda etapa del proyecto se podría implementar la opción de bloqueo de IPs que son constantemente notificadas como atacantes, esto se debe a que muchos clientes al recibir la notificación podrían tomar medidas, pero algunos otros pueden no realizar acción alguna y con esto, seguir siendo una IP causante de problemas en la red, una mejor alternativa para la misma seria el bloqueo.

3. Está surgiendo un protocolo llamado SDEE, desarrollado para la comunicación de eventos generados por dispositivos de seguridad. A futuro se espera que cualquier DPI pueda ser capaz de comunicarse a través de este protocolo. Esto podría mejorar la forma de obtención de la información de los diferentes dispositivos de seguridad utilizados en el proyecto y aumentar otros más sin que consuma tiempo en investigación de cómo funciona el mismo.

VIII. BIBLIOGRAFIA

[1] Check Point SmartWorkFlow [En línea] <http://www.checkpoint.com/products/smartworkflow-software-blade/index.html > [Consultado: 7 Enero 2011]

[2] Spam [En línea] <http://es.wikipedia.org/wiki/Spam> [Consultado: 7 Enero 2011]

[3] Spam [En linea] <http://www.colombiadigital.net/noticias-tic/noticias/noticias-de-la-ccd/993-aumenta-la-cantidad-de-correos-maliciosos-en-internet.html> [Consultado: 7 Junio 2011]

[4] Anatomia de una Botnet [En línea] <http://www.malwarecity.com/blog/anatomy-of-a-botnet-196.html> [Consultado: 7 Enero 2011]

[5] Bots y Botnet una amenza creciente [En línea] <http://mx.norton.com/theme.jsp?themeid=botnet > [Consulta: 8 Enero 2011]
[6] Botnets [en línea] <http://mrcracker.com/2009/09/botnet/> [Consulta: 8 Enero 2011]
[7] ¿Qué es un ataque DDoS? [En línea] <http://thecustomizewindows.com/2011/05/what-is-ddos-attack/ > [Consultado: 7 Enero 2011]
[8] DIPLOMA: Distributed Policy Enforcement Architecture for MANETs [En línea] <http://www.cs.columbia.edu/~angelos/Papers/2010/diploma.pdf> [Consultado: 7 Enero 2011]
[9] Syn Flodding [En línea] <http://searchsecurity.techtarget.com/definition/SYN-flooding> [Consultado: 8 Enero 2011]
[10] UDP flood attack [En línea] <http://en.wikipedia.org/wiki/UDP_flood_attack> [Consultado: 8 Enero 2011]
[11] Port Scanning Techniques [En Línea] <http://nmap.org/book/man-port-scanning-techniques.html> [Consultado: 9 de Enero 2011]
[12] Sandvine [En línea] <http://www.sandvine.com/> [Consultado: 10 Enero 2011]
[13] ASA [En línea] <http://www.cisco.com/en/US/products/ps6120/index.html > [Consultado: 8 Enero 2011]
[14] ADM AGM [En línea] <http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6236/product_data_sheet0900aecd80220a6e.html> [Consultado: 10 Enero 2011]
[15] UCEPROTECT [En línea] <http://www.uceprotect.net/en/index.php > [Consultado: 12 Enero 2011]