ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

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

TESINA DE SEMINARIO

Previo a la obtención del Título de:

INGENIERÍA EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN SISTEMAS DE INFORMACIÓN

INGENIERÍA EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN SISTEMAS TECNOLÓGICOS

INGENIERÍA EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN SISTEMAS DE INFORMACIÓN

Presentado por:

PETTER BYRON CASTRO TIGRE

NOEMÍ DE LOS ANGELES MONTESDEOCA CORREA

GEORGE ENRIQUE REYES TOMALÀ

GUAYAQUIL – ECUADOR

2011

AGRADECIMIENTO

Agradeciendo a Dios todopoderoso, a mi familia que brindó su apoyo incondicional, y a todos los docentes que me nutrieron de conocimientos y valores los cuales ayudaron a alcanzar este objetivo.

Petter Castro T.

Ante todo a mi Dios Todopoderoso que día a día ha estado junto a mi abriendo puertas y guiándome en cada decisión a tomar. A mi madre, una mujer luchadora, si no me hubiese inspirado con su tenacidad no hubiese podido cumplir este sueño. A José Mendoza, quien recorrió el largo camino de la vida universitaria conmigo siendo mi soporte y ayuda, antes como enamorado y hoy en mi vida profesional como mi esposo. A mis maestros, a mis compañeros, a mis jefes y mis familiares que abrieron la puerta cuando llegue a esta ciudad.

Noemí Montesdeoca C.

A Dios que me ha guiado cada día de mi vida, a mi Mamá, Papá y mi familia que siempre me están apoyando en todo.

George Reyes Tomalá

TRIBUNAL DE SUSTENTACIÓN

_____

Msc. Alfonso Aranda S.

PROFESOR DEL SEMINARIO DE GRADUACIÓN

_____

Msc. Ignacio Marín García

DELEGADO DEL DECANO DE LA FACULTAD

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesina de Seminario, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

(Reglamento de Graduación de la ESPOL).

Petter Castro Tigre **Noemí Montesdeoca Correa**

George Reyes Tomalá

RESUMEN

El presente proyecto muestra el desarrollo de un sistema para la ayuda en la toma de decisiones en base a lacorrelación de eventos en base a alertas de seguridad, logs de equipamientos CISCO y Linux, y otros parámetros.

Esta herramienta constara 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.

En el Capítulo 1 se expone el planteamiento del problema que el presente proyecto de tesis busca solucionar, además indica cuales será los objetivos a cubrir por el mismo.

En el Capítulo 2 se revisan los fundamentos teóricos respecto a los tráficos maliciosos, se hablaran acerca de algunas herramientas utilizadas para discernir el trafico sospechoso y se indican los objetivos y el alcance del proyecto.

En el capítulo 3 se el diseño de nuestro sistema donde detallamos la arquitectura, los requerimientos mínimos para que nuestro sistema posea un optimo funcionamiento y la plataforma en la que fue desarrollado.

En el capítulo 4 se detalla la implementación del sistema en mención, es decir la forma en que se maneja la administración del aplicativo, los scripts que se utilizan para las diferentes tareas y la forma de realizar la correlación de la información.

En el capítulo 5 se realizan las mediciones y se analizan los resultados de las pruebas realizadas en la red comparando la metodología manual contra los resultados arrojados por la herramienta desarrollada.

ABREVIATURAS

ACK (Acknowledgement) Acuse de recibo.

Mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado. Si el terminal de destino tiene capacidad para detectar errores, el significado de ACK es "ha llegado y además ha llegado correctamente".

ADM (Anomaly Detector Module) Modulo detector de anomalías.

Modulo de servicio integrado de CISCO que ayuda a defender los recursos de internet de la empresa de ataques DDoS.

AGM (Anomaly Guard Module) modulo protector de anomalías.

Modulo de servicio integrado de CISCO que ayuda a detectar los recursos de internet de la empresa de ataques DDoS.

AJAX (Asynchronous JavaScript and XML).

Técnica de desarrollo web para crear aplicaciones interactivas. Estas aplicaciones se ejecutan en el cliente, es decir, en el navegador de los usuarios mientras se mantiene la comunicación asíncrona con el servidor en segundo plano.

AS (Autonomous system) Sistema Autónomo.

Es un grupo de IPs operadas por una o más operadores de red las cuales tienen una única política de enrutamiento externa. Los protocolos de

enrutamiento externos son usados para intercambiar información de enrutamiento entre ASes.

ASN (Autonomous System Number) Número de Sistema Autónomo.

Un AS público tiene un número único global, un ASN, asociado a él. Este número es usado para intercambiar información de enrutamiento externa y como un identificador del AS.

DDoS (Distributed Denial of Service) Ataque Distribuido de Denegación de Servicio.

Ampliación del ataque DoS el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

DHTML (Dynamic HTML) HTML Dinámico.

Conjunto de técnicas que permiten crear sitios web interactivos utilizando una combinación de lenguaje HTML estático, un lenguaje interpretado en el lado del cliente (como JavaScript), el lenguaje de hojas de estilo en cascada (CSS) y la jerarquía de objetos de un DOM.

DOM (Document Object Model) Modelo en Objetos para representación de documentos.

Interfaz de programación de aplicaciones (API) que proporciona un conjunto estándar de objetos para representar documentos HTML y XML, un modelo estándar sobre cómo pueden combinarse dichos objetos, y una interfaz estándar para acceder a ellos y manipularlos.

DPI (Deep Packet Inspection) Inspección profunda de paquetes.

Es el acto de inspección realizado por cualquier equipo de red de paquetes que no sea punto final de comunicación, utilizando con algún propósito el contenido que no es el encabezado del paquete.

IME (IPS Manager Express)

Aplicación ofrecida por CISCO la cual provee un sistema de monitoreo, seguimiento de problemas y generador de reportes de ataques realizados en la red del cliente.

ISP (Internet Service Provider) Proveedor de servicio de internet.

Empresa que brinda conexión a Internet a sus clientes.

IT Tecnología Informática.

Estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras.

LAN (Local Área Network) Red de Área Local.

Red que conecta los ordenadores en un área relativamente pequeña y predeterminada.

MARS (Monitoring, Analysis and Response System) Sistema de monitoreo análisis y respuesta.

Herramienta de Cisco que permite monitorear y mitigar los ataques en la red.

MTA (Message Transfer Agent) Agente de Transferencia de Mensajes.

Es un sistema organizado de correo electrónico que se encarga de recibir los mensajes desde diversos lugares y distribuirlos entre los usuarios.

MVC (Model View Controller) Modelo Vista Controlador.

Patrón de arquitectura de software que separa los datos de una aplicación, la interfaz de usuario, y la lógica de control en tres componentes distinto.

POP (Post Office Protocol) Protocolo de la oficina de correo

Protocolo estándar de internet usado por programas de e-mail locales para recibir e-mails desde un servidor remoto a través de una .conexión TCP/IP.

PTS (Policy Traffic Switch) Comutador política y tráfico.

Dispositivo de control de políticas e inspección en la red.

RAM (Random Access memory) Memoria de acceso aleatorio.

Es la memoria en la cual el procesador recibe las instrucciones y guarda los resultados.

SDEE (Security Device Event Exchange)

Protocolo desarrollado para la comunicación de eventos generados por dispositivos de seguridad.

SSH (Secure Shell) Intérprete de ordenes seguras.

Nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico para poder ejecutar programas gráficos.

SLA (Service Level Agreement) Acuerdo de nivel de servicio.

Contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

SYN (Synchronize) Sincronizar.

Es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales de una conexión en el procedimiento de establecimiento de tres fases (3 way hand shake).

TCP/IP (Transmission Control Protocol/Internet Protocol) Protocolo de Control de Transmisión/Protocolo de Internet

Es un conjunto de protocolos que proporcionan transmisión fiable de paquetes de datos sobre redes.

UDP Protocolo de Datagrama del Usuario.

Protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión.

VPN (Virtual Private Network) Red privada virtual.

Red de comunicaciones de área ancha provista por una portadora común que suministra aquello que asemeja líneas dedicadas cuando se utilizan, pero las troncales de base se comparten entre todos los clientes como en una red pública.

WAN (Wide Area Network) Red de Area Amplia.

Red de computadoras de gran tamaño, generalmente dispersa en un área metropolitana, a lo largo de un país o incluso a nivel planetario LAN.

GLOSARIO

Adware

Programa que automáticamente se ejecuta, muestra o baja publicidad web al computador después de instalar el programa o mientras se está utilizando la aplicación.

Algoritmo

Secuencia de pasos para resolver un problema.

Arquitectura cliente-servidor

Consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta. Aunque esta idea se puede aplicar a programas que se ejecutan sobre una sola computadora es más ventajosa en un sistema operativo multiusuario distribuido a través de una red de computadoras.

Blogs

Es un sitio web actualizado periódicamente, que recopila textos y artículos de uno o varios autores.

Botnet

Botnet es un conjunto de bots o zombies (computadores infectados) que se ejecutan de forma autónoma y automática bajo el control de una persona (bot máster) usualmente para desarrollar tareas maliciosas.

Bugs, bicho, insecto

También conocidos como holes o agujeros. Defecto en un software o un hardware que no ha sido descubierto por los creadores o diseñadores de los mismos.

Carrier

Empresa encargada de proveer tecnología de información.

CERT

Es una organización dedicada a velar para que las tecnologías apropiadas y las prácticas de gestión de los sistemas sean usadas para resistir los ataques a los sistemas en red para limitar el daño y asegurar la continuidad de servicios críticos, en lugar de ataques exitosos, accidentes o averías.

CheckPoint

Empresa la cual esta dedica a ofrecer soluciones de seguridad para los proveedores tecnología de información.

Cisco

Es una empresa encargada de la fabricación, ventas, mantenimiento y consultoría de equipos de comunicación.

Crackers

Persona que viola la seguridad de un sistema informático con fines de beneficio personal o para hacer daño.

Crimeware

Tipo de programa de computadora diseñado específicamente para cometer crímenes del tipo financiero, intentando pasar desapercibido por la víctima.

Escalable

Propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para extender el margen de operaciones sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

Firewall, Cortafuegos

Dispositivo o conjunto de dispositivo diseñado para permite o denegar transmisiones en la red basándose en reglas.

Framework, Ventana de Trabajo

Estructura conceptual y tecnológica definida, que sirve para desarrollar y organizar programas informáticos.

Frontend

Parte del software que interactúa con el o los usuarios.

Gusano

Es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos casi siempre causan problemas en la red mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

Hacker

Experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar *hackeo* y *hackear* a las obras propias de un hacker.

Honeypot

Un servidor diseñado para ser atacado y que actúa como señuelo para hackers los cuales piensan que se conectan a un verdadero sistema informático y actúan sobre él, permitiendo así a su propietario monitorizar la actividad del "pirata" con distintos fines: estudiar su comportamiento, fijar los puntos débiles de su red, etc.

Host(Huésped)

Computadores conectados a la red, que proveen y/o utilizan servicios a/de él.

Javascript

Lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos,3 basado en prototipos, imperativo, débilmente tipado y dinámico.

Linux

Sistema operativo que utiliza un núcleo diseñado por Linux y que es de código abierto.

Malware

También llamado badware viene de la palabra (malicious software) programa malicioso, es un programa que se infiltra sin consentimiento del propietario para obtener datos o dañar el computador.

Multiplataforma

Esto significa que el hardware o software que es multiplataforma tiene la característica de funcionar de forma similar en distintas plataformas (distintos sistemas operativos por ejemplo).

Mysql

Sistema de gestión de bases de datos relacional, multihilo y multiusuario.

Perl

Lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado shell (sh), AWK, sed, Lisp y, en un grado inferior, de muchos otros lenguajes de programación.

Phishing

Se denomina phishing a la práctica de usar mails fraudulentos o copias de sitios web fraudulentos con el fin de extraer datos financieros de usuarios para propósitos de robos de identidad.

PHP(Hypertext Preprocessor)

Lenguaje interpretado de alto nivel embebido en páginas HTML y ejecutado en el servidor.

Plataforma

Determinado software y/o hardware con el cual una aplicación es compatible y permite ejecutarla.

Procesos Batch

Llevar a cabo una operación particular de forma automática.

Rootkit

Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers con el objetivo de acceder ilícitamente a un sistema informático.

Script(Archivo de procesamiento por lotes)

Programa usualmente simple, que por lo regular se almacena en un archivo de texto plano. Los script son casi siempre interpretados, pero no todo programa interpretado es considerado un script. El uso habitual de los scripts es realizar diversas tareas como combinar componentes,

interactuar con el sistema operativo o con el usuario. Por este uso es frecuente que los shells sean a la vez intérpretes de este tipo de programas.

Sniffers

Es un analizador de paquetes, este programa captura trama de una red de computadores.

Spam

Se denomina spam a los mensajes no solicitados, no deseados o de remitente no conocido generalmente de tipo publicitario que suelen afectar al receptor.

Spammer

Personas o empresas dedicadas a la transmisión de correos o mensajes no deseados o spam.

Spamtrap

Es un honeypot usada para recolectar datos de los spammers.

Spyware(Programa Espía)

Programa que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Symfony

Framework a utilizarse para el desarrollo, basado en php diseñado para optimizar, gracias a sus características, el desarrollo de las aplicaciones web.

Troyano

Programa malware capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recompilar información o controlar remotamente a la máquina de algún usuario, pero sin afectar el funcionamiento de ésta.

Virus

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO 1

Planteamiento del problema

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 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 Descripción de la Solución Propuesta

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.

1.3 Soluciones Alternativas

En el mercado se puede conseguir varios sistemas y plataformas que ayudan y controlan la seguridad en redes, pero estos productos requieren de una inversión económica superior. Algunos de ellos son:

Monitoring, Analysis and Response System (MARS) que provee CISCO permite: identificar las amenazas de aprendizaje de la topología, configuración y el comportamiento del entorno de red; facilita la solución de problemas, la identificación de ataques o vulnerabilidades para una amplia gama de redes empresariales; visualmente caracteriza a una ruta de ataque, identifica la fuente de amenaza, y hace recomendaciones precisas para la mitigación de amenazas y simplifica la gestión de incidentes y la respuesta mediante la integración con Cisco Security Management.

Existen otras herramientas como el RAS EnVisio, una plataforma que permite la interacción con algunos tipos de dispositivos, específicamente dispositivos de marca CISCO, firewall de marca CheckPoint y registro de servidores

Microsoft Windows; dentro de esas tres clasificaciones esta herramienta es muy flexible, permite realizar correlaciones y reportes.

La fuerte inversión financiera que estas soluciones alternativas conllevan y la estricta dependencia de marcas específicas para que estos tengan un correcto funcionamiento, hacen que nuestro sistema sea superior antes ellas.

1.4 Objetivo General

Desarrollar un sistema integral, disminuyendo el proceso que un administrador de red realiza, reduciendo así los gastos operativos relacionados con el tráfico malicioso. Adicionalmente este sistema detectará el equipo infectado y notificará al responsable de la red al que pertenece el equipo.

1.5 Objetivos específicos

- Identificar y comprender que tipos de ataques reconocen cada uno de las fuentes de detección.
- Analizar y explicar en lenguaje natural lo que cada fuente de detección muestra en sus registros.
- Correlacionar los datos obtenidos de la fuente, descartando falsos positivos e identificando las

incidencias y las consecuencias que las mismas han tenido en la red.

- Proporciona una interfaz web muy intuitiva, que se admite diferentes vistas de estadísticas y “Top 10” de la red global.
- Implementar un sistema integrado que emita notificaciones al cliente y al técnico encargado de la seguridad.

1.6 Alcance

El alcance de este proyecto es el cumplimiento de los objetivos específicos implementados y debidamente probado en un ambiente controlado. Ver Capítulo 5 (Pruebas y Resultados).

CAPITULO 2

Fundamentos Teóricos.

En el Capítulo 1 se definió el problema del tráfico malicioso en una red pero breves rasgos, en el presente capitulo hablaremos sobre cada uno de las ataques que nuestra red se encuentra expuesta y algunas de las herramientas utilizadas para realizar dichos ataques.

2.1 Definición: Seguridad Informática y Tráfico Malicioso

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.

2.2 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.

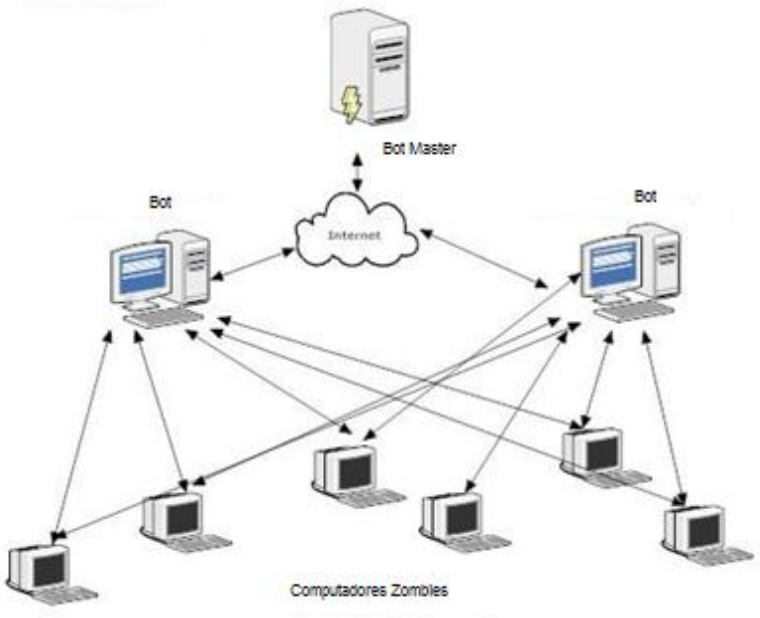


Figura 2.1 Forma de ataque de una Botnet[6]

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.

Hay muchos tipos de servicios que bloquean estas direcciones. Pero los más importantes realizan el bloqueo por IP y algunos otros bloquean por rangos de IP. Los que bloquean por rangos de IP investigan primero cual es el rango de IP que tiene la compañía (basándose en la IP que encontraron haciendo Open Relay), y bloquean dicho rango.

Los blogs o cadenas de mensajes son utilizados para obtener las direcciones de correos electrónicos y luego estos sean enviados hacia una fuente la cual realiza el envío indiscriminado de mails. Existen varias motivos por los cuales el envío de spam se vuelve atractivo o rentable para los spammers, ya que mediante ellos pueden enviar anuncios publicitarios o incluso llegar a infectar un ordenador y poder instalarse como un sniffer para capturar el trafico de paquetes con la finalidad de obtener información valiosa tal como claves de tarjetas de crédito.

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

2.3 Ataque de Denegación de Servicio (DoS)

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]

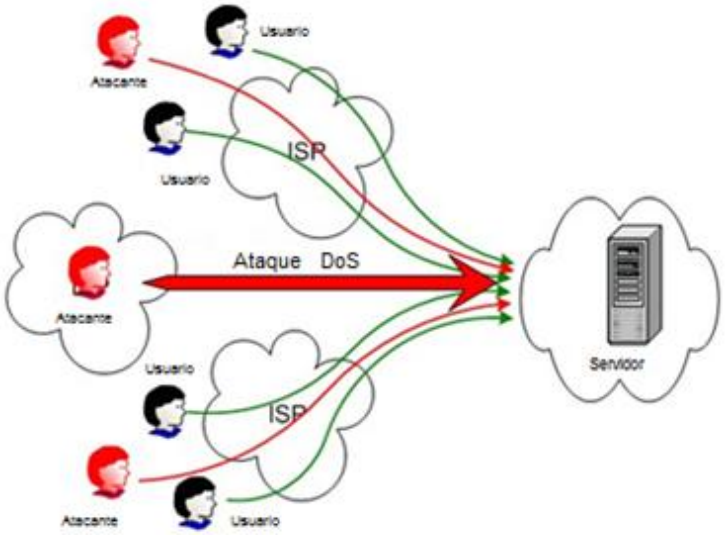


Figura 2.2 Ataque DoS[7]

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.

Existen muchas formas de realizar de ataques de DoS a continuación mencionaremos algunas de estas:

- ***Inundación SYN (SYN Floods)*** es una manera de realizar un ataque de denegación de servicio, un inundación por SYN se define cuando una o varias maquinas envía muchas peticiones SYN a un servidor para sobrecargarlo y dejarlo fuera de servicio, el paquete syn es utilizado para realizar un three way hand shake por el protocolo TCP para poder iniciar una sesión entre cliente y servidor.[9]

- ***Inundación de Flujo (Flow Floods)*** este ataque es muy similar a la inundación de *Syn,* la diferencia radica en que este utiliza una gran flujo paquetes que son enviados de uno o varios computadores que puede ser desde una botnet que va tratar de conectarse con un servidor especifico para realizar un ataque DoS.

- ***Usuario de ancho de banda (User Bandwidth)*** es otra variante de un ataque DoS, este ataque implica varios usuarios de una aplicación que se encuentran comprometidos por una virus o gusanos que tratan de sobrecargar de datos a un servidor, por consecuencia hace que el servicio se vuelva lento o se quede no

disponible porque el ancho de banda no da para más requerimientos debido a la congestión.

- ***Flujo UDP (UDP Floods)*** es un ataque que utiliza el protocolo UDP, el atacante envía muchos paquetes UDP a un puerto específico de manera aleatoria. Debido a que el sistema no conoce el destinatario, responderá como destino inalcanzable a la IP origen que la mayoría de veces es falsa para ocultar la identidad del atacante. Este ataque aprovecha la ausencia del control de flujo de dicho protocolo.[10]

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.

2.4 Herramientas y Soluciones para Detección de Tráfico Malicioso

Actualmente existen muchas herramientas y soluciones que permiten a las empresas administrar mejor la seguridad en sus redes. Como se indico en el Capítulo 1, 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. 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).

- **ASA**

  La serie ASA de Cisco son equipos de Seguridad de Redes los cuales integran una combinación de tecnologías en una única plataforma para la detección de amenazas y ataques que sufren las redes. Detiene

los ataques antes de que entren a la red, controlan la actividad y proveen conectividad VPN flexible. [13]

Además, como punto importante, la conexión de estos dispositivos varía de acuerdo a las necesidades del cliente, pero en condiciones normales estos se deben ubicar entre el enrutador con acceso hacia el internet y el servidor de la compañía tal como se muestra en la figura 2.3, y de esta forma cualquier trafico malicioso desde el internet sea detenido antes que acceda al servidor y pueda perjudicar la red.

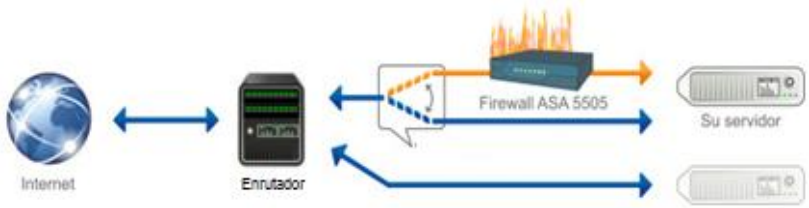


Figura 2.3 Diagrama de Funcionamiento de ASA[12]

- **Modulo protector de anomalías (Anomaly Guard Module)**

  Módulo propio 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).

  Cuando el ADM identifica un posible ataque, avisa al módulo de Cisco AGM para comenzar un desvío

dinámico, que vuelve a dirigir el tráfico destinado a los recursos objeto y única y luego sea inspeccionado una vez más. Todo el resto del tráfico continúa fluyendo directamente a su destino. [14]

- **Modulo detector de anomalías (Anomaly Detector Module)**

  El ADM es un módulo de servicios integrados de Cisco Catalyst 6500 y 7600 que ayuda a proteger a las grandes organizaciones contra la negación distribuida de servicio (DDoS) o la red de otros ataques, permitiendo a los usuarios iniciar rápidamente la mitigación servicios y bloquear los ataques antes de negocio se ve afectada. [13]

  ADM utiliza la última tecnología de análisis de comportamiento y el reconocimiento de ataques para detectar todo tipo de ataques en línea. Con la constante supervisión del tráfico con destino a un dispositivo de protección, como una web de comercio electrónico o servidor de aplicaciones.

  El ADM compila perfiles detallados que indican cómo los dispositivos se comportan bajo "condiciones de funcionamiento normales". Si el ADM detecta cualquier desviación, se considera a este comportamiento anómalo como un ataque potencial y responde en

función de las preferencias del usuario mediante el envío de una alerta para iniciar una respuesta manual, mediante la activación de un sistema de gestión, o mediante el lanzamiento del AGM para comenzar de inmediato los servicios de mitigación.

- **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.

- **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] Cada uno de los ataques registrados por el sitio puede ser de 3 tipos:

  Nivel 1: IPs/32, es decir IPs especificas las cuales generaron los ataques. Para que una IP sea detectada

y asignada a este nivel se necesitan varias razones las cuales pueden ser:

- Es una IP detectada por los spamtraps.
- La IP atacante intentó hacer un port scanning previo al envío de spam.
- El ataque fue realizado contra los servidores de este sitio.

A este nivel aunque se considera la frecuencia de los ataques un factor importante, lo es también si la IP generadora del ataque se encuentra dentro de una red la cual ha venido realizando ataques con anterioridad. En este caso, basta con que se detecte una vez, para que la IP sea inmediatamente registrada como posible spammer.

Nivel 2: Se puede decir que si varias IPs dentro de una misma red, realizan ataques continuos de spam, la mayor parte de la red está comprometida. Debido a esto, este nivel en lugar de registrar IPs/32, registra aquellos “bloques de IPs” o “asignaciones” desde las cuales se han producido un número considerable de ataques de Nivel 1. Para que una red pueda ser considerada de nivel 2 se considera lo siguiente:

- Las asignaciones menores a /26 serán escaladas a nivel 2 inmediatamente como se detecte una IP de nivel 1.
- Las asignaciones con /25 serán escaladas a nivel 2 inmediatamente como se detecten dos IPs de nivel 1.
- Las asignaciones con /24 serán escaladas a nivel 2 inmediatamente como se detecten cuatro IPs de nivel

Nivel 3: Este nivel es el más extremo y puede llevar a bloquear varias IPs y registrarlas como falsos positivo, debido a que se registran todas las IPs correspondientes a un ASN, siempre que existan más de 100 IPs o un 2% de IPs en Nivel 1.

CAPITULO 3

Diseño del sistema

En este capítulo se presentan las herramientas usadas en el desarrollo del sistema, la arquitectura y los requerimientos mínimos de la aplicación, así como los diferentes algoritmos implementados para la extracción de los datos de las fuentes de información.

3.1 Arquitectura de la Aplicación

En el sistema se utiliza la arquitectura cliente – servidor, si bien es cierto que esta arquitectura es una de la más antiguas, también es cierto que es una de la más utilizadas y aún en la actualidad muchas empresas de gran prestigio utilizan este esquema.

3.2 Requerimientos Mínimo de Hardware

Para el correcto funcionamiento de la aplicación, el mismo debe ser montado en un servidor con procesador Intel, 1Gb memoria RAM o superior y disco duro con una capacidad de 50Gb. Los indicados son requerimientos mínimos; sin embargo, mientras mejor sea el hardware mejor será el rendimiento de la aplicación.

3.3 Plataforma de Desarrollo

El framework utilizado para el desarrollo del sistema se fundamenta en Symfony como solución multiplataforma, la cual nos ayudó a optimizar el desarrollo de la aplicación haciendo uso del patrón MVC, permitiéndonos realizar un sistema escalable y fácil de adaptarse a cambios en la implementación del mismo.

3.4 Recopilación de los Datos y Centralización de la Información

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.

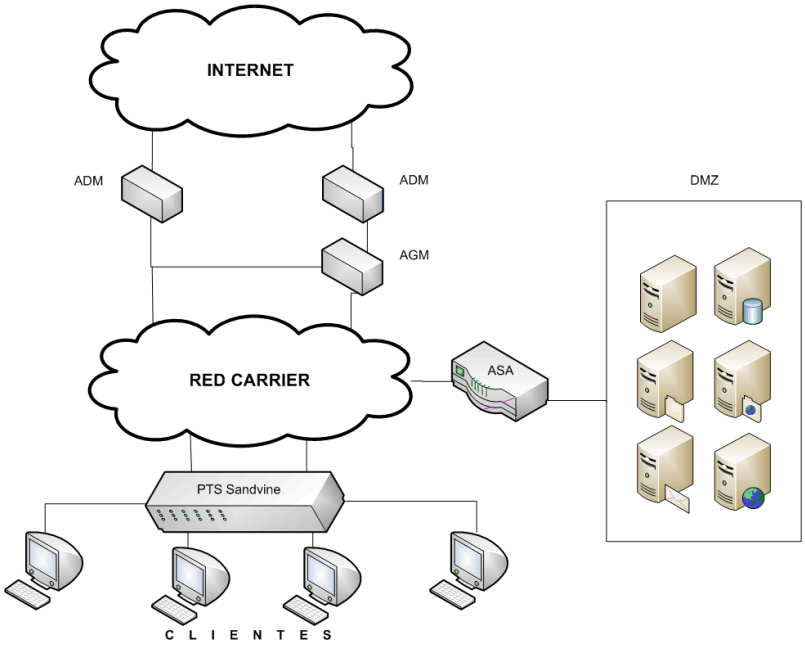


Figura 3.1 Esquema de la red

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.

En el **Anexo B** 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 (Para ver el diagrama completo de la base de todos ir a Anexo A). A continuación, mostraremos cuales son los ataques que cada fuente detecta y las tablas donde se almacena esta información:

En la herramienta ***SANDVINE***, 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 víctima, tiempo que duro el ataque, fecha detectado, el tipo de ataque y el protocolo que utiliza.

En la herramienta ***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. Para nuestra investigación escogeremos ciertas firmas relevantes de este firewall ya que no todas utilizaremos en el proyecto:

- **ICMP Network Sweep w/Echo:** Esta firma se activa cuando un barrido de la red se está ejecutando por medio de paquetes ICMP.
- **TCP SYN Host Sweep:** Se activa cuando varios paquetes syn son enviados en la red desde un solo host.
- **TCP SYN Port Sweep:** Se activa cuando varios paquetes TCP syn fragmentados son enviados a numero de puertos destinos en un host.
- **UDP Bomb:** Se active cuando las cabeceras de los paquetes UDP están mal formados y significa que un ataque de denegación de servicio puede estar en curso.
- **Open SSL SSL/TLS Malformed Handshake DoS:** Esta firma se activa cuando un paquete TLS three-way handshake que llega al puerto TCP posee un formato incorrecto esto indica que un ataque de denegación de servicio está en curso.
- **Grumbot:** Se activa cuando detecta muchos mensajes (Spam) saliendo de un mismo host.
- **MSSQL Resolution Service Stack Overflow:** Esta firma se activa cuando hay un intento de desbordamiento del buffer en el puerto 1434 esto indica que un ataque de denegación de servicio está en curso.
- **Oracle BEA WebLogic Server Apache Connector Buffer:** Se active cuando la vulnerabilidad de Oracle WebLogic Server es explotada esto es indicio que una

atacante quiere obtener el control de nuestro servidor remotamente.

En base a que acción describe cada una de las firmas indicadas anteriormente, podemos agruparla las actividades detectadas en la red de la siguiente manera.

- **DoS**: UDP Bomb, OpenSSL/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 event_table_1 en nuestra base local y así 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 dispositivos que 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 vía 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.

Un ataque puede durar varios minutos o incluso horas, para obtener los datos el operador debería seguir los siguientes pasos:

1) Mediante el comando <show>, el cual permite ver cuáles son las ips que están siendo atacadas (Figura 3.2).

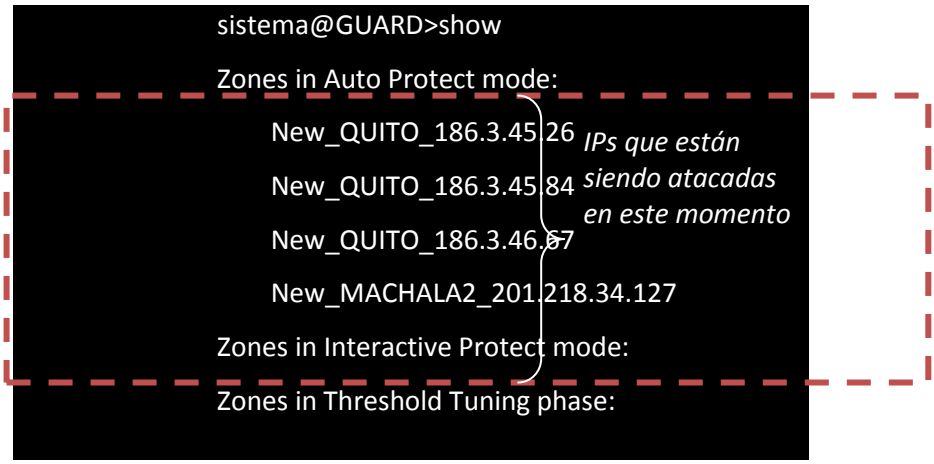


Figura 3.2 Resultado del comando show en AGM

2) Para la obtención de los detalles acerca de este ataque, ejecutamos el siguiente comando <*show zone New_MACHALA2_201.218.34.127 dynamic-filters details*>, Figura 3.3, obteniendo la siguiente información:

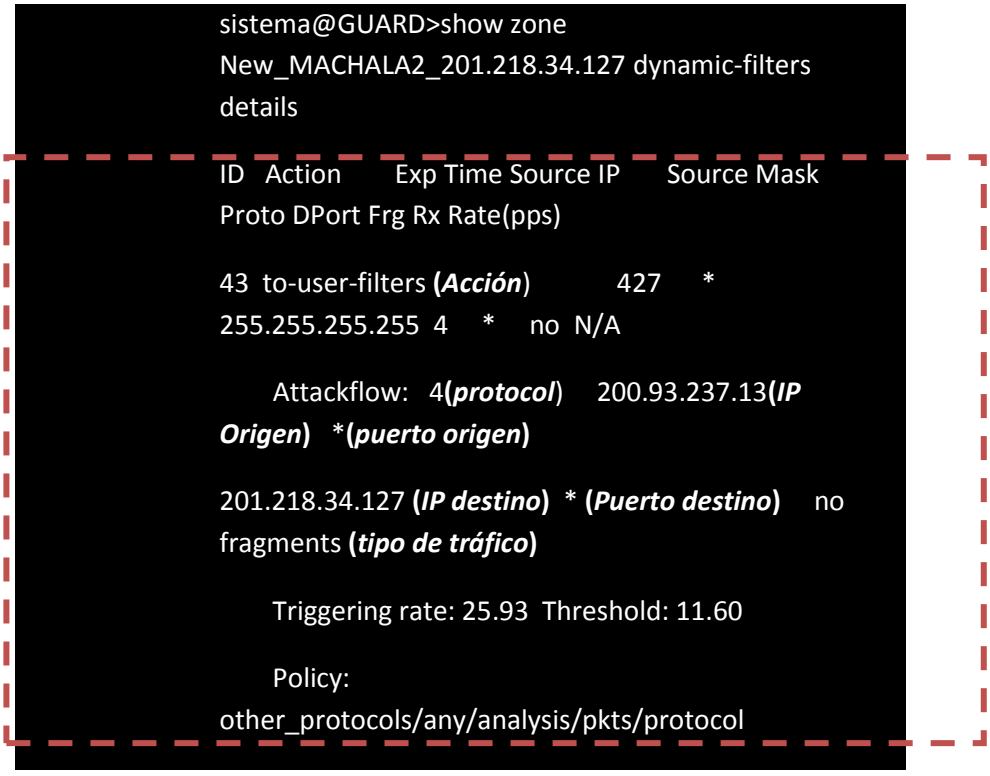


Figura 3.3 Resultado del comando show zone en AGM

Para la obtención de los datos proporcionados por el AGM, se utiliza un script realizado en PERL. Perl consta de un módulo especial llamado Net::SSH::Expect, el cual permite la interacción por vía SSH a diferentes dispositivos. El script ingresa a la base del SRC los datos de la IP atacada y en mismo se mantiene activa mientras la IP este siendo atacada en el AGM.

El script lee esta información y refresca la base de datos cada cierto tiempo determinado, y con esta información se realiza la correlación con las otras fuentes de información.

Los **correos enviados por centros de seguridad de información reconocidos**, contiene información de IPs que han sido encontradas como infectadas por algún tipo de malware y son reportados a una cuenta de correo especial, esta 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.

El algoritmo funciona de la siguiente manera:

1. El script se conecta al RELAY SMTP vía SSH.
2. Una vez dentro el script lee todos los correos cuyos remitentes sean conocidos como direcciones de CERT conocidos.
3. Cada centro tiene su formato de envío de información, varían tanto en el asunto como en el cuerpo; se toma la información relevante basado en plantillas conocidas de estos remitentes.
4. La información obtenida en el punto 3 es guardada en la base de datos del SRC para que el mismo pueda utilizarlo en los scripts de correlación.

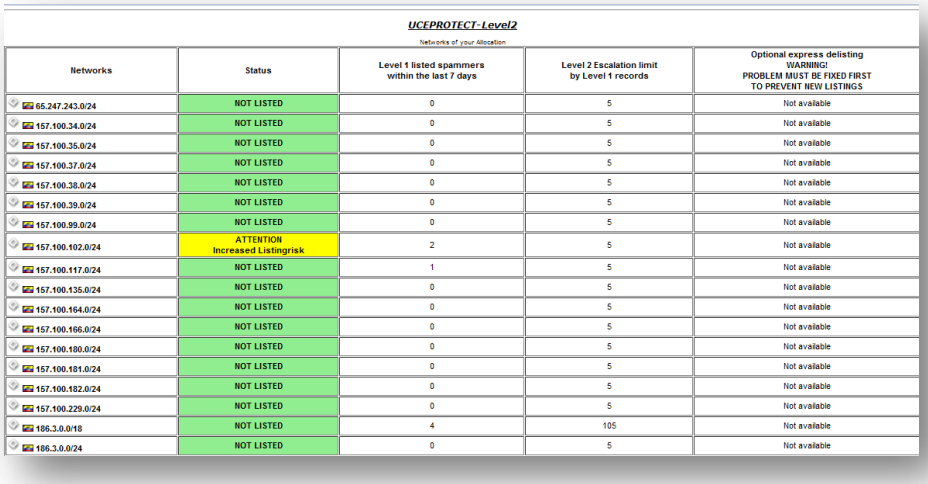
La tabla donde se almacena esta información es llamada correo y tiene la siguiente información: ip atacante, remitente, cuerpo (para soporte) y fecha de detección del spammer.

En el caso del sitio ***UCEPROTECT®*** el cual nos provee de direcciones IP o bloques de IPs las cuales son consideradas como propagadoras de spam, pero, aunque es una fuente la cual tiene su inteligencia y nos provee cierta información de los ataques, no es suficiente para cumplir nuestro objetivo y es necesario aplicar inteligencia propia para saber qué datos

son relevantes para nuestro estudio y poder discernir para obtener resultados fiables con un alto grado de confianza.

Debido a esto, antes de empezar a analizar el acceso a los datos, examinaremos que datos de los que nos provee esta fuente son considerados relevantes y por qué lo son; para esto UCEPROTECT nos facilita dos tipos de información de nuestro interés:

a) ASN.- Muestra las asignaciones es decir todos los ataques de Nivel 2 de las cuales se están enviando spam hacia la red.



UCEPROTECT-Level2

Networks of your Allocation

Networks	Status	Level 1 listed spammers within the last 7 days	Level 2 Escalation limit by Level 1 records	Optional express delisting WARNING! PROBLEM MUST BE FIXED FIRST TO PREVENT NEW LISTINGS
65.247.243.0/24	NOT LISTED	0	5	Not available
157.100.34.0/24	NOT LISTED	0	5	Not available
157.100.35.0/24	NOT LISTED	0	5	Not available
157.100.37.0/24	NOT LISTED	0	5	Not available
157.100.38.0/24	NOT LISTED	0	5	Not available
157.100.39.0/24	NOT LISTED	0	5	Not available
157.100.99.0/24	NOT LISTED	0	5	Not available
157.100.102.0/24	ATTENTION Increased Listingrisk	2	5	Not available
157.100.117.0/24	NOT LISTED	1	5	Not available
157.100.135.0/24	NOT LISTED	0	5	Not available
157.100.164.0/24	NOT LISTED	0	5	Not available
157.100.166.0/24	NOT LISTED	0	5	Not available
157.100.180.0/24	NOT LISTED	0	5	Not available
157.100.181.0/24	NOT LISTED	0	5	Not available
157.100.182.0/24	NOT LISTED	0	5	Not available
157.100.229.0/24	NOT LISTED	0	5	Not available
186.3.0.0/18	NOT LISTED	4	105	Not available
186.3.0.0/24	NOT LISTED	0	5	Not available

Figura 3.4 Resultados por ASN

Analizando la Figura 3.4 se pueden visualizar cinco columnas, pero solamente las cuatro primeras son de interés para el análisis las cuales se refieren a lo siguiente:

Networks.- Lista la subred o asignación desde la cual se está realizando el ataque, se incluye la dirección de la subred y la máscara de la misma.

Level 1 listed spammers within the last 7 days.- Indica cuantas incidencias de Nivel 1 se han realizado dentro de la respectiva asignación en los últimos 7 días. Para objeto de análisis y simplificación en la terminología, a esta columna la denominaremos “Ataques de Lvl 7-1”.

Level 2 Escalation limit by Level 1 records.- Indica el número total de incidencias de Nivel 1 realizadas desde la asignación respectiva. Para objeto de análisis y simplificación en la terminología, a esta columna la denominaremos “Ataques de Lvl X-1”.

Status.- Indica el estado de atención que se debe considerar a esta subred, pudiendo tomar 3 diferentes valores:

- NOT LISTED.- Cuando a pesar de que es una asignación detectada en Nivel 2, se han detectado menos de la mitad del número de ataques de Nivel 1 permitidos para la subred en los últimos 7 días.
- INCREASED LISTINGRISK.- Cuando se han detectado la mitad de las incidencias de Nivel 1 permitidas para la subred en los últimos 7 días.

- HIGH LISTINGRISK.- Cuando se ha detectado más de la mitad de las incidencias de Nivel 1 permitidas para la subred en los últimos 7 días.

Como ejemplo para análisis de cada una de las columnas y su respectivo significado conjunto, vamos a ver el primero registro observado en la Figura 3.4.

La asignación detectada como spammer me lo indica la columna “Networks” que en este caso particular tiene como valor al bloque 65.247.243.0/24. Al tener como mascara /24, para que la asignación haya podido escalar al nivel 2, es necesario que como mínimo se detecten 4 ataques de Nivel 1, este valor me lo indica la columna “Ataques de Lvl X-1” la cual en este caso me indica un valor de 5, excediendo al mínimo permitido para la subred y registrándolo en Lvl 2 automáticamente. La columna “Status” me indica el nivel de atención que le debemos dar a esta red, en este caso me indica NOT LISTED debido a que en los últimos 7 días no se ha registrado ningún ataque de Nivel 1. (Ataques de Lvl 1 7-1).

b) La segunda información que nos brinda el UCEPROTECT es un repositorio de todas las IPs/32 las cuales han registrado ataques en la red y son considerados como spammers (Figura 3.5).

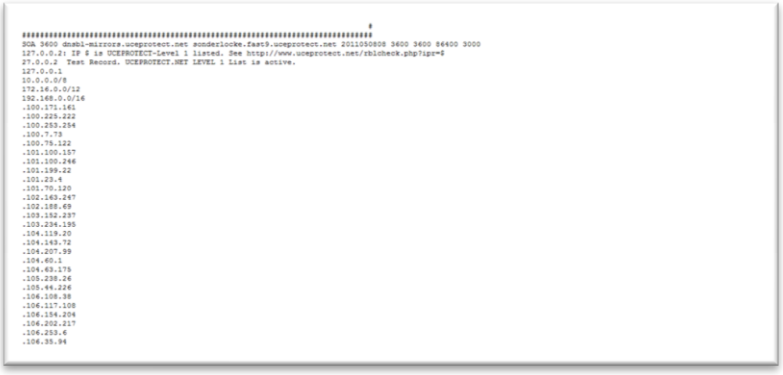


Figura 3.5 Repositorio IPs

Luego de conocer cuáles son los datos que podemos obtener a partir de esta fuente, lo siguiente a realizar es tomar solamente los datos de interés que ayuden a cumplir con el objetivo del proyecto, para finalmente ver la forma de acceso a cada uno de ellos.

Como se pudo apreciar en la figura 3.5, podemos obtener las asignaciones las cuales podrían estar comprometidas, pero el problema es que tomamos a todas estas como spammers, generando una gran cantidad de falsos positivos, debido a que existe el riesgo de que bloqueemos a todo un bloque de IPs.

Es por esto que el análisis no contemplara toda la lista generada en este sitio, sino que, para que un registro sea considerado, deberá tener el status en Increased Listingrisk o High ListingRisk.

Luego de obtenidas las asignaciones en estos Status, se procede a buscar las IPs relacionadas a esa subred dentro del repositorio de IPs que nos brinda el sitio, para conocer la dirección exacta que realizo el ataque, dándoles a estas una criticidad alta y a las demás direcciones de la misma subred, una criticidad media, ya que aunque no han sido identificadas como spammers, pueden llegar a serlo si el comportamiento de la asignación persevera.

Existen 2 formas de recoger los datos, una para cada una de las fuentes de información que nos brinda el sitio, es decir por medio del ASN o el repositorio de IPs.

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.

CAPITULO 4

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.

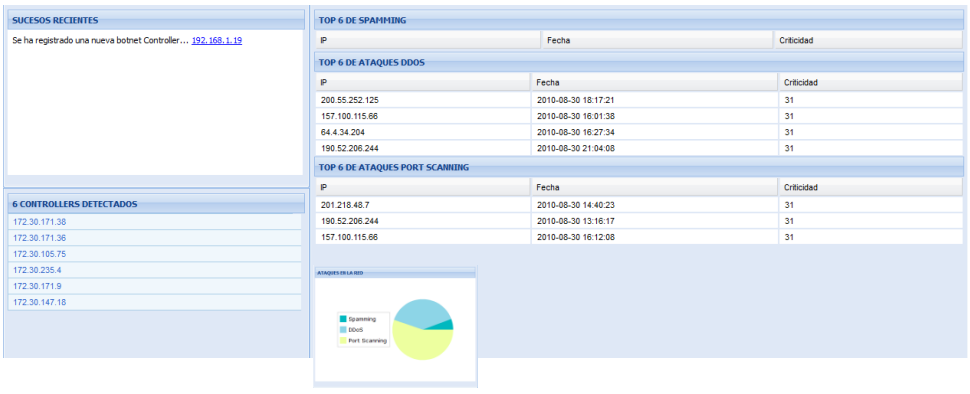


Figura 4.1 Interfaz de Usuario

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.

4.3 Correlación de la Información

Después de tener todos los eventos en nuestra base de datos se realiza la respectiva correlación entre IPs atacantes de las fuentes Sandvine y ADM/AGM de un mismo tipo ataque en este caso ataques de DoS. Se selecciona un rango de fecha (5 minutos). Una vez que se obtengan los ataques que cumplan las condiciones antes mencionadas se guardaran en la tabla ataque. Se obtiene los identificadores de los registros correlacionado en este caso de Sandvine y ADM/AGM, si poseen una ip victima en común se la

guardara, caso contrario se la podrá obtener por medio de sus respectivo registros en Sandvine y ADM/AGM, la fecha detectado es el momento que estas se están correlacionado y la criticidad se la coloca como baja debido a que solo son dos fuentes correlacionándose.

La correlación de tipo Spam se la realiza entre las fuentes Sandvine, Correo, Uceprotect por ip atacante igual que el algoritmo anterior se obtiene los datos de hoy y se los recorre con intervalos de 5 minutos para luego ser almacenado en la base. Obteniendo los identificadores de cada fuente y almacenándolos, la criticidad varía por la cantidad de fuentes correlacionada, ejemplo si es Sandvine, Correo, y Uceprotect al mismo tiempo esta será criticidad media y si son 2 fuentes será baja.

4.4 Identificación del atacante

Luego de haber encontrado la correlación, se debe encontrar la entidad que produjo el ataque y almacenarlo en la base. Esto se lo realiza gracias a que se puede relacionar esa IP con el atacante a través de una base fuente que registra el nombre de la persona y la ip asignada a esta. Las dos formas de reconocer el cliente al que corresponde esa IP dentro de la base son:

- IP WAN/LAN.- Cuando la IP se encuentra directamente registrada como una de las interfaces de algún CPE.
- IP de subred.- Cuando la IP no se encuentra directamente registrada en la base de datos remota, sino que pertenece a una subred registrada en ella.

En caso de que la IP detectada no coincida con ninguna de las opciones anteriores, se concluye que es un ataque proveniente de una red externa a la empresa y se queda registrado de esa forma.

4.5 Notificación al Encargado del Equipo Infectado y/o Atacante

Luego de haber realizado la correlación de eventos se procede a notificar al atacante acerca del delito el cual está cometiendo, siempre y cuando este se encuentre registrado como cliente del proveedor de servicios que está utilizando nuestro sistema. Esta notificación incluye la IP desde la cual se está realizando el ataque, la fecha en que se realizo y una breve explicación de la causa del problema en lenguaje natural.

4.6 Script obtención de posibles Botnet

Para la obtención de posibles Botnet se utiliza la fuente asa, se obtienen los registros de con tipos ataque port scanning y

se los agrupa por ip, luego se cuentan los ataques y se seleccionan las 10 con más ataques de este tipo y se la coloca como ip controladora, luego a cada ip victima de estas ip se las registra como posible bot y en expansión Botnet se ingresan cada uno de los ataques a estas víctimas. Este proceso se ejecutara cada 12 horas.

CAPITULO 5

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 este capítulo 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.

5.1 Ambiente donde se realizará las pruebas

Para las pruebas, se tuvo la ayuda de una empresa que provee servicio de internet, por lo tanto, las mismas fueron controladas y debidamente monitoreadas por el encargado de la red de la empresa que facilito su infraestructura; este ambiente constó de:

a) El servidor SRC, el mismo que ejecutaba los scripts según se encuentren programados en el crontab. Estos scripts se conectaban a los diferentes dispositivos para recolectar la información según los mecanismos definidos ya en la sección anterior.
b) Los dispositivos: el PTS de SANDVINE, el IDEM de ASA, el firewall AGM y el POP de la empresa en mención, estuvieron constantemente monitoreados por el administrador de la red, cerciorándose que los scripts ejecuten solamente las acciones que deben ejecutar, tal que no pudiesen causar inconvenientes en los mismos.

5.2 Detalle de las pruebas y resultados

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	11seg
2	Tiempo en colocar parámetros de búsqueda en el sistema	33seg
3	Tiempo de respuesta	17seg
TOTAL TIEMPO		**57seg**

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	58seg
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 14seg
5	Tiempo que tomo en realizar la correlación de la información obtenida	2 min 49 seg
TOTAL TIEMPO		**13 min 15seg**

Tabla 5.3.- Tiempos Escenario 2- Proceso Manual.

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

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 encontraba 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	58seg
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 39seg
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	8seg
2	Tiempo en colocar parámetros de búsqueda en el sistema	19seg
3	Tiempo de respuesta	18seg
TOTAL TIEMPO		**35seg**

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

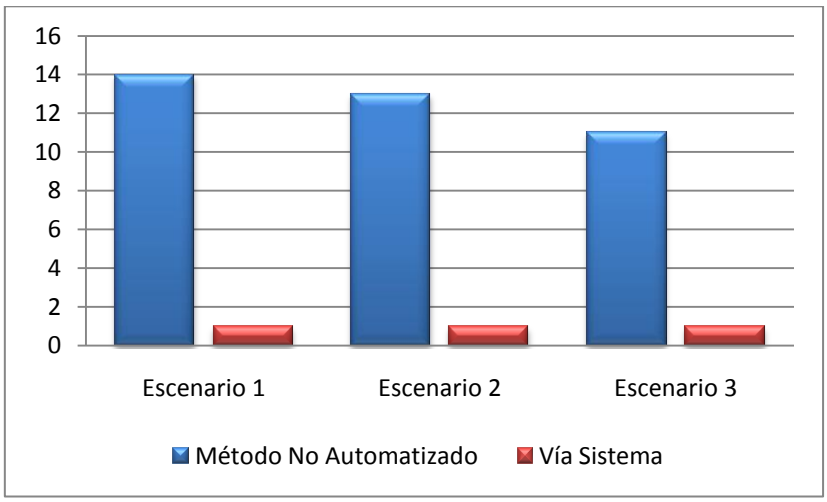


Figura 5.1.- Escenario 1 comparación de tiempo.

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.

VIA SISTEMA		
1	Tiempo en conectarse al Sistema	9seg
2	Tiempo en colocar parámetros de búsqueda en el sistema	38seg
3	Tiempo de respuesta	47seg
TOTAL TIEMPO		**1 min 34seg**

Tabla 5.7.- Tiempos Escenario 4- Resultados Obtenidos por Sistema.

CONCLUSIONES

Una vez concluido el Sistema Automatizado 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 eventos maliciosos suscitados en la red, 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 eventos 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 de nuestra 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.

RECOMENDACIONES

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

1. 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.
2. Se puede aumentar la visibilidad y el control de la seguridad de la red aumentando fuentes de detección heterogéneas.

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.

BIBLIOGRAFIA

[1] Check Point Software Technologies Ltda., Check Point SmartWorkFlow, http://www.checkpoint.com/products/smartworkflow-software-blade/index.html, fecha de consulta enero 2011

[2]Nassiel, Spam, http://es.wikipedia.org/wiki/Spam,fecha de consulta enero 2011

[3]Symantec Corporation, Spam, http://www.colombiadigital.net/noticias-tic/noticias/noticias-de-la-ccd/993-aumenta-la-cantidad-de-correos-maliciosos-en-internet.html, fecha de consulta junio 2011

[4] Bogdan Botezatu, Anatomía de una Botnet, http://www.malwarecity.com/blog/anatomy-of-a-botnet-196.html, fecha de consulta enero 2011

[5]Symantec Corporation, Bots y Botnet una amenaza creciente, http://mx.norton.com/theme.jsp?themeid=botnet, fecha de consulta enero 2011

[6]MrCracker, Botnets, http://mrcracker.com/2009/09/botnet/,fecha de consulta enero 2011.

[7] Abhishek Ghosh, ¿Qué es un ataque DDoS?, http://thecustomizewindows.com/2011/05/what-is-ddos-attack, fecha de consulta enero 2011

[8] Alicherry Mansoor y Keromytis Angelos, DIPLOMA: Distributed Policy Enforcement Architecture for MANETs, http://www.cs.columbia.edu/~angelos/Papers/2010/diploma.pdf,fecha de consulta enero 2011

[9] Tech Target®, SynFlodding,http://searchsecurity.techtarget.com/definition/SYN-flooding, fecha de consulta enero 2011

[10] Software Engineering Institute, UDP flood attack, http://en.wikipedia.org/wiki/UDP_flood_attack,fecha de consulta enero 2011

[11] Lyon Gordon, Port Scanning Techniques,http://nmap.org/book/man-port-scanning-techniques.html, fecha de consulta enero 2011.

[12] Sandvine Corporation, Sandvine, http://www.sandvine.com, fecha de consulta enero 2011.

[13] CISCO System Inc, ASA, http://www.cisco.com/en/US/products/ps6120/index.html, fecha de consulta enero 2011.

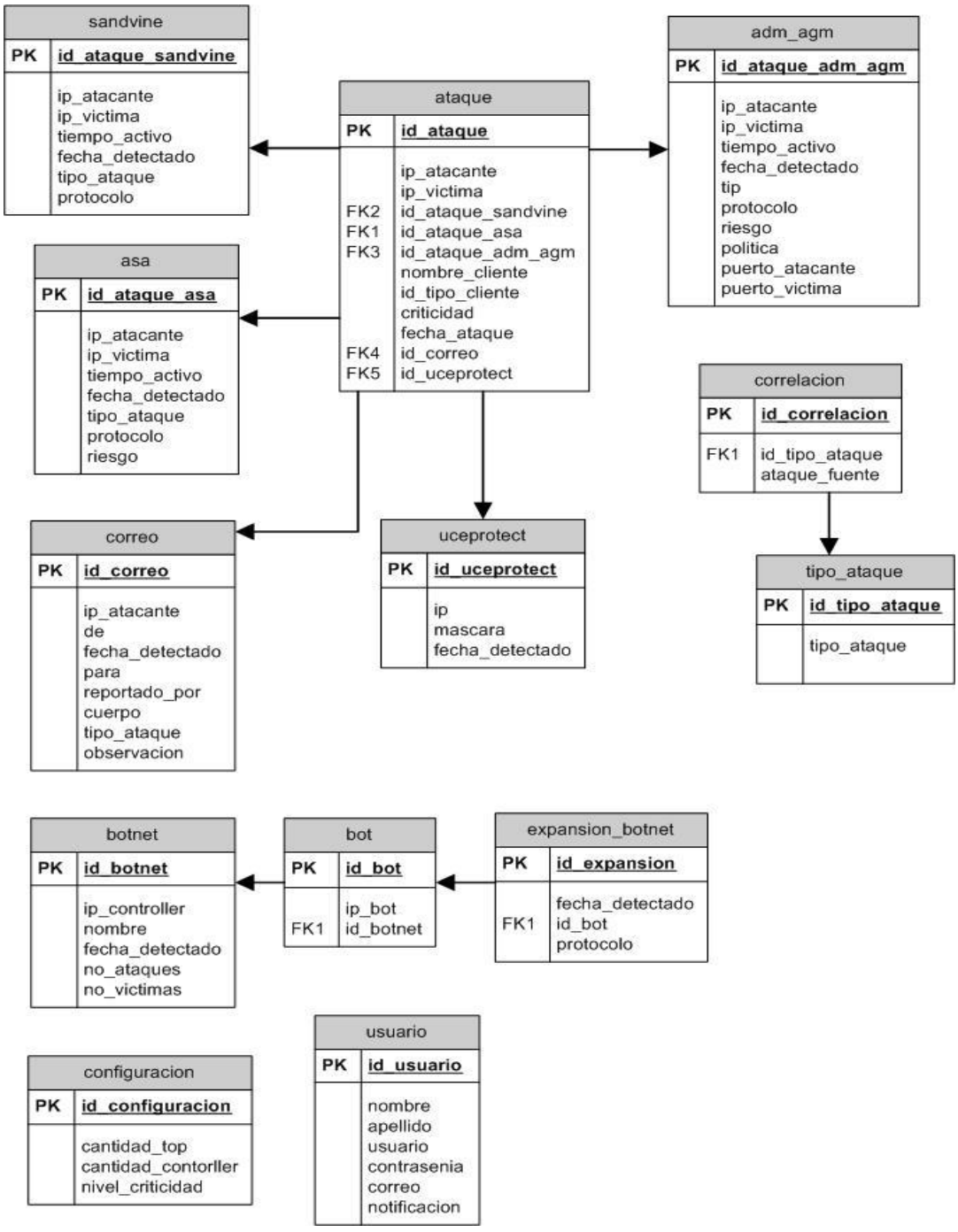
[14] CISCO System, ADMAGM, http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6236/product_data_sheet0900aecd80220a6e.html, fecha de consulta enero 2011

[15] UCEPROTECT-Orga, UCEPROTECT, http://www.uceprotect.net/en/index.php, fecha de consulta enero 2011

ANEXOS

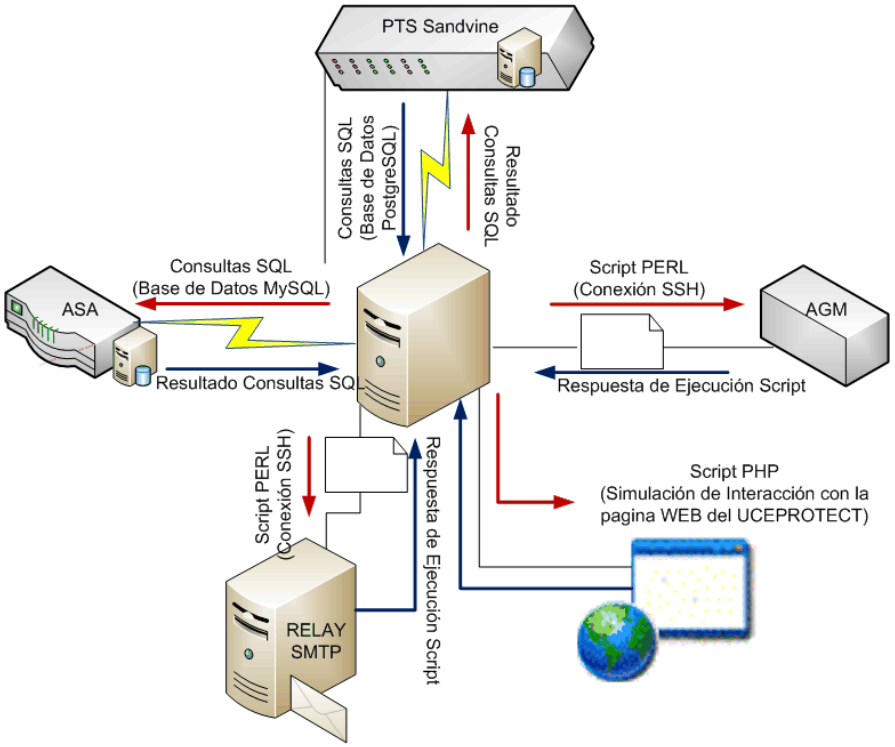
ANEXO A

Modelo Lógico de la Base de Datos



ANEXO B

Esquema completo de las fuentes de detección.



ANEXO C

Manual de Usuario.

1. Introducción

Este manual ha sido elaborado con la finalidad de ofrecer la información necesaria para el uso del sistema “DEXTER”, para facilitar la interacción y permitirle al usuario conocer el significado de cada una de las pantallas. Con el fin de facilitar la comprensión de este documento, se añaden capturas de pantallas del sistema.

2. Requerimientos Básicos

- Tener instalado un navegador de internet con soporte para javascript.
- Tener usuario y clave de acceso para el sistema.
- Conexión a la VPN para poder acceder al aplicativo.

3. Objetivo

El principal objetivo de este documento es:

“Ayudar y guiar en el uso del sistema mediante una descripción detallada e ilustrada de las pantallas”.

4. Ingreso al Sistema

Para ingresar en el sistema el usuario debe realizarlo con su usuario y contraseña el cual ya debió haber sido registrado (Figura 1.1). En caso de aun no tenerlo se lo debe solicitar por correo a la cuenta del administrador del sistema.

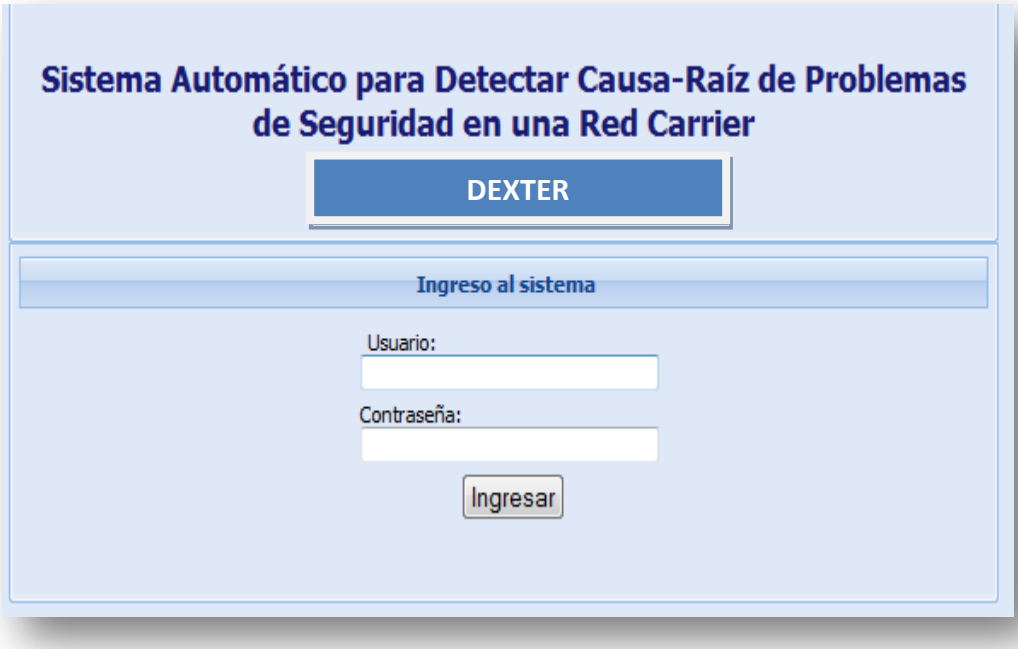


Figura 1.1 Ingreso al Sistema

5. Pantalla principal

Una vez dentro del sistema, la página principal lista varios paneles los cuales muestran un resumen en tiempo real de la situación en la red (Figura 1.2).

- **Sucesos recientes.-** En este panel se encuentran sucesos ocurridos en la red actualizados cada 20 minutos con la finalidad de dar a conocer al usuario, los

ataques que están ocurriendo casi que en tiempo real para que puedan tomar las medidas necesarias de control.

- **Ataques TOP.-** Muestran las IPs con mas cantidad de ataques diarios realizados en las diferentes clasificaciones tales como Spam, Ataque DoS y Port Scanning, y con la respectiva criticidad de alta, media y baja; donde alta indica que fue detectada por la mayor cantidad de fuentes de detección.
- **Controller.-** En este panel se encuentra la actividad de las posibles botnet obtenidas por el comportamiento en la red. Estas aparecen en orden descendente con respecto a la cantidad de ataques que están realizando en la red.

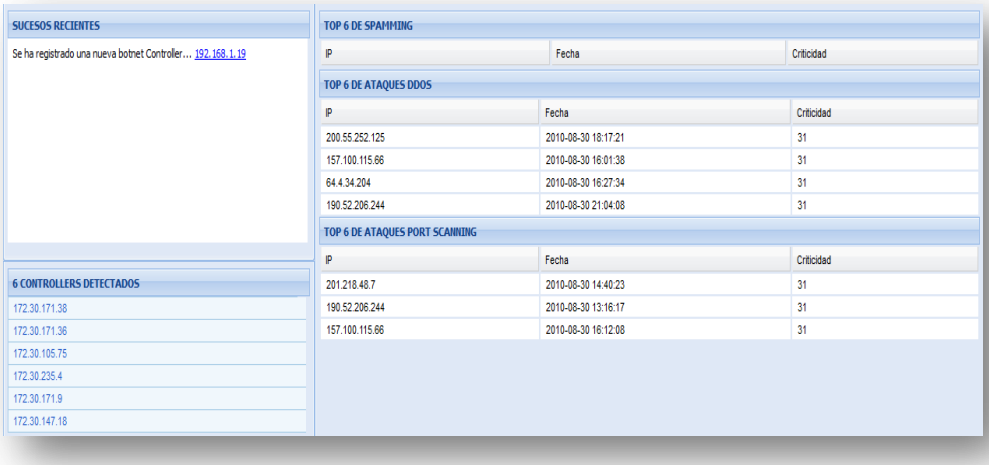


Figura 1.2 Pantalla Principal

6. Información de IP considerada parte de una Botnet

Al dar clic sobre uno de los registros del panel de Controller, se lista la información correspondiente a esa IP considerada como parte de la botnet o comúnmente denominados bots (Figura 1.3), tal como:

- Gráficamente se visualiza el comportamiento de esa IP en el transcurso de la semana indicando la cantidad de ataques que ha realizado.
- En la parte inferior de la grafica se expone lo mismo de la grafica de una forma más detallada, es decir agregando el número exacto de ataques que realizo esa IP en esa fecha y el numero de IPs victimas a las cuales ha estado atacando.

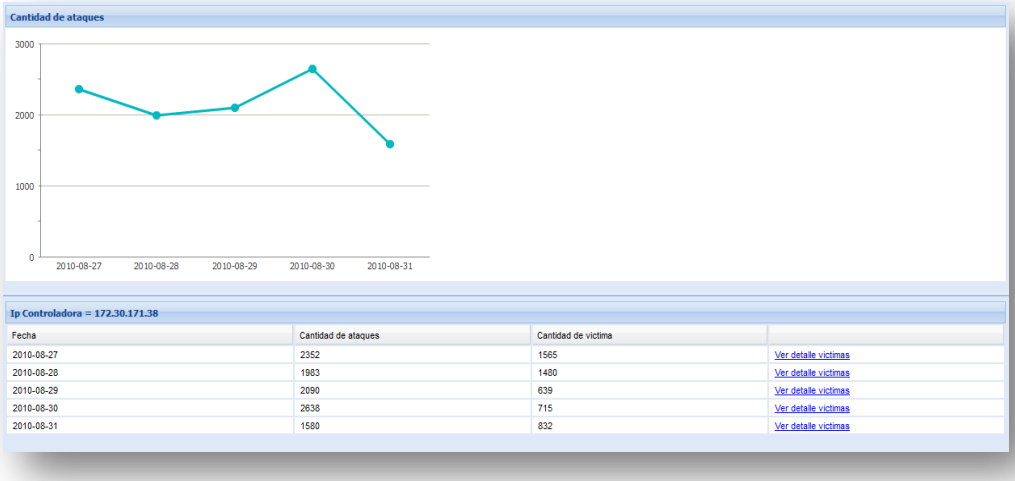
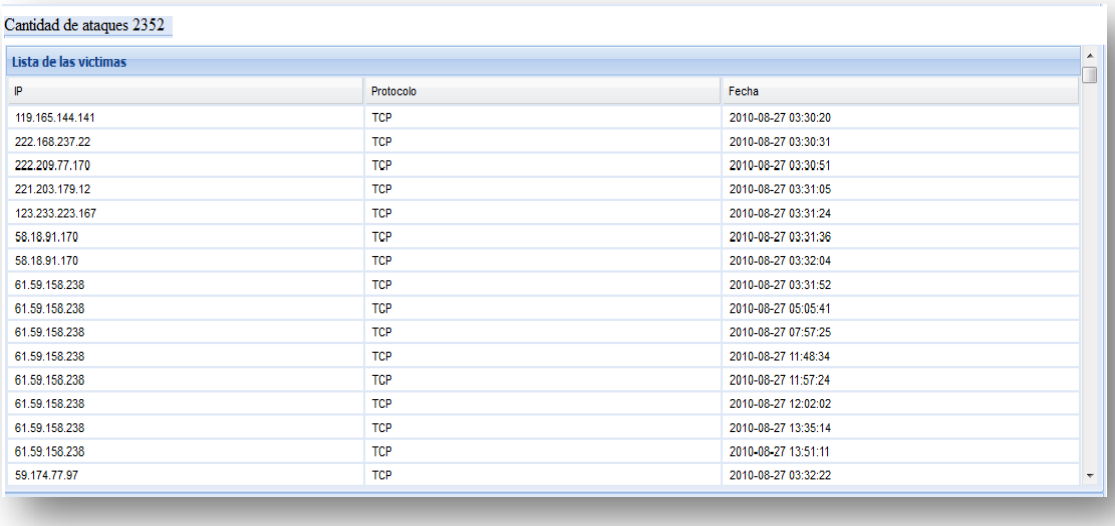


Figura 1.3 Información de IP considerada parte de una Botnet

7. Detalle de ataque de posible bot

En la Figura 1.3 se pudo observar que existe un enlace por cada día de la semana en que se han detectado ataques de esa bot. Al hacer clic sobre ese enlace se nos presentan todos los ataques realizados ese día específico, con fecha, hora e IP a la cual se le realizo el ataque (Figura 1.4).



Cantidad de ataques 2352

Lista de las victimas

IP	Protocolo	Fecha
119.165.144.141	TCP	2010-08-27 03:30:20
222.168.237.22	TCP	2010-08-27 03:30:31
222.209.77.170	TCP	2010-08-27 03:30:51
221.203.179.12	TCP	2010-08-27 03:31:05
123.233.223.167	TCP	2010-08-27 03:31:24
58.18.91.170	TCP	2010-08-27 03:31:36
58.18.91.170	TCP	2010-08-27 03:32:04
61.59.158.238	TCP	2010-08-27 03:31:52
61.59.158.238	TCP	2010-08-27 05:05:41
61.59.158.238	TCP	2010-08-27 07:57:25
61.59.158.238	TCP	2010-08-27 11:48:34
61.59.158.238	TCP	2010-08-27 11:57:24
61.59.158.238	TCP	2010-08-27 12:02:02
61.59.158.238	TCP	2010-08-27 13:35:14
61.59.158.238	TCP	2010-08-27 13:51:11
59.174.77.97	TCP	2010-08-27 03:32:22

Figura 1.4 Detalle de Ataques del Bot

8. Pastel de ataques en la red

Haciendo referencia a la Figura 1.2, también se puede observar un panel el cual nos muestra gráficamente cual es el tipo de ataque con mayor incidencias sobre la red en el día (Figura 1.5).

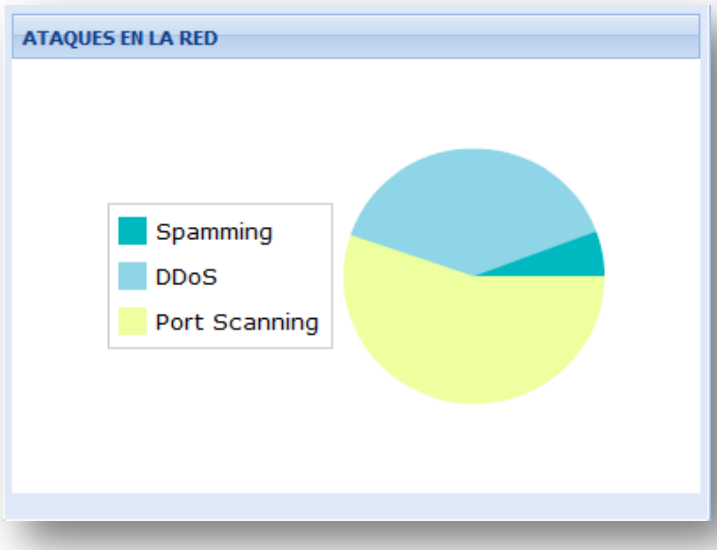


Figura 1.5 Pastel de Ataques en la red

9. Ataques diarios

Al hacer clic sobre uno de los ataques mostrados en el pastel de la Figura 1.5, podemos obtener los detalles de cuantos ataques se han realizado en el transcurso del dia, permitiendo filtrarlos por la frecuencia (1, 2 o 4 horas) o por la criticidad de los ataques realizados en ese día (Figura 1.6).

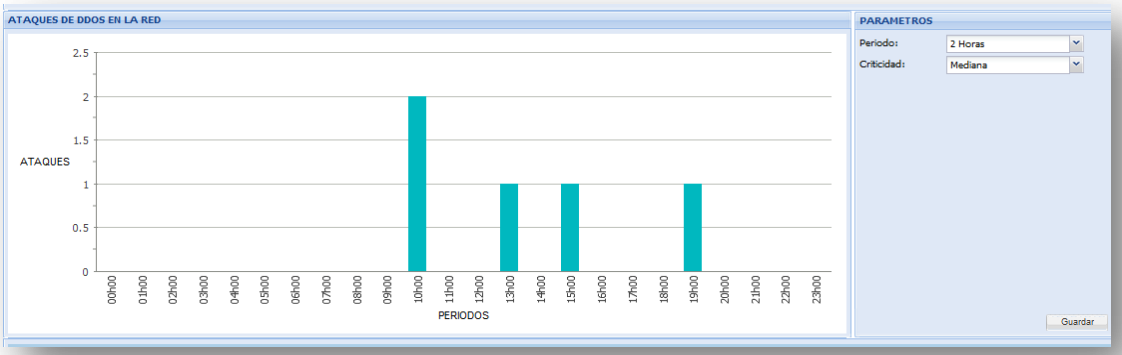


Figura 1.6 Ataques diarios

10. Administración de usuarios

Finalmente existe la opción de administración de usuario, en la cual se puede crear o editar usuarios para permitir el ingreso al sistema. Los datos necesarios son el nombre, apellido, email, recibir notificaciones, el usuario y la contraseña de ingreso al sistema (Figura 1.7).

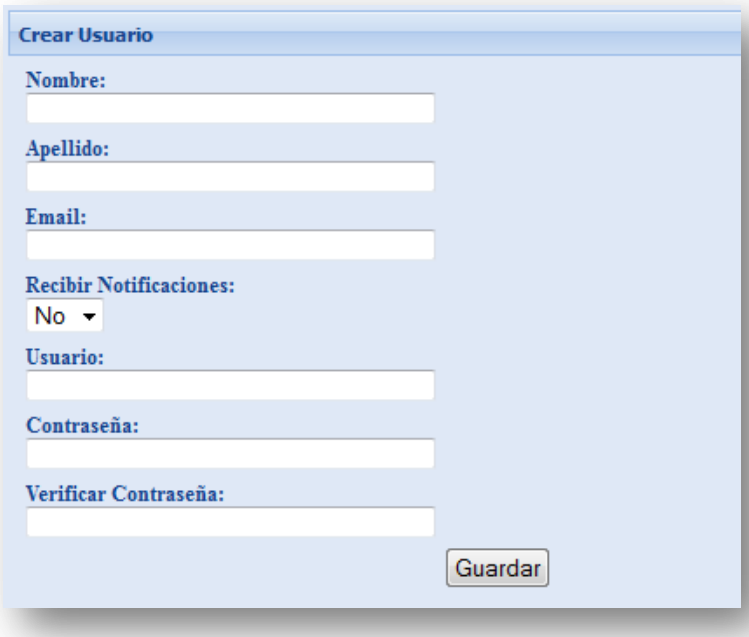


Figura 1.7 Administración de usuarios

ANEXO D

Manual de Instalación

Requisitos

- Sistema Operativo Unix con Distribución Centos
- Apache 2.2.3 o superior (levantar el servicio)
- PHP 5.3 o superior
- Mysql 5.0 (levantar el servicio)

Pasos de Instalación

- Crear la base de datos llamada **malware** y proceder a restaurar sobre esta, el archivo **malware.sql** adjunto.

```
mysql -u root -p malware <malware.sql
```

- Montar el proyecto Malware sobre el directorio /home/

- Agregar las siguientes líneas al final del archivo httpd.conf ubicado en /etc/httpd/conf/

```
<VirtualHost *:80>
ServerName malware.telconet.net
DocumentRoot "/home/Malware/web"
DirectoryIndexindex.php
  Alias /sf /home/Malware/web/sf
ErrorLog "/var/log/httpd/error_log"
<Directory "/home/Malware/web">
AllowOverride All
    Allow from All
</Directory>
<Directory "/home/Malware/web">
AllowOverride All
    Order allow,deny
    Allow from All
</Directory>
<Directory "/home/Malware/web/sf">
AllowOverride All
    Order allow,deny
    Allow from all
```

```
</Directory>
</VirtualHost>
```

- Ubicarse dentro del directorio del proyecto y ejecutar el siguiente comando:

```
symfony cc
```

- Ubicar la carpeta scripts dentro del directorio /home/

- Abrir el crontab mediante el comando **crontab –e** y agregar las siguientes líneas

```
5 * * * *   /usr/bin/php  “/home/scripts/Migracion/ASA/index.php”
5 * * * *   /usr/bin/php  “/home/scripts/Migracion/UCE-PROTECT/index.php”
5 *  * * *  /usr/bin/php  “/home/scripts/Migracion/SANDVINE/index.php”
5 *  * * *  /usr/bin/php  “/home/scripts/Migracion/ADM-AGM/index.pl”
5 *  * * *  /usr/bin/php  “/home/scripts/Migracion/CORREOS/index.pl”
6 * * * *   /usr/bin/php  “/home/scripts/Correlacion/correlacion.php”
* 12 * * * /usr/bin/php  “/home/scripts/Botnet/botnet.php”
024 * * * /usr/bin/php  “/home/scripts/Notificacion/notificacion_clientes.php”
```