ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UNA PLATAFORMA DE DETECCIÓN DE ACCESOS A SITIOS MALICIOSOS"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

IVETTE KEMBELY CARRERA MANOSALVAS

GUAYAQUIL - ECUADOR

AÑO: 2016

AGRADECIMIENTO

A Dios, por brindarme salud; a mis padres, por cada sabio consejo; a mi Esposo e Hija, por su apoyo y amor incondicional, por darme las fuerzas necesarias para lograr mis objetivos y por quienes nace mi deseo de superación; a mis compañeros de la Maestría por su amistad incondicional y por la lucha constante para culminar esta meta.

Ivette Carrera Manosalvas

DEDICATORIA

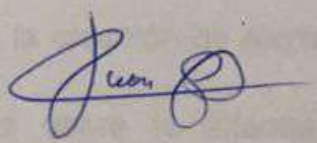
A cada una de las personas que contribuyeron en mi formación profesional, brindándome una sólida formación a través de sus conocimientos y experiencias permitiéndome contribuir al progreso del país.

Ivette Carrera Manosalvas

TRIBUNAL DE SUSTENTACIÓN

MGS. Lenin Freire C.

DIRECTOR MSIA



MGS. Juan Carlos García P.

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

RESUMEN

El presente trabajo muestra la implementación de una plataforma de detección de accesos a sitios maliciosos en un ambiente de prueba previamente configurado.

En el primer capítulo se detalla el problema a resolver así como la solución propuesta. Posteriormente se procede a aclarar conceptos teóricos necesarios para la ejecución del proyecto.

En el tercer capítulo se específica paso a paso las instalaciones y configuraciones que se deben realizar tanto en el servidor proxy como en el servidor Splunk, así como también la configuración del proxy en la máquina que simula el usuario. Para la creación de alertas, primero se explica como realizar búsquedas básicas sobre la información indexada para luego proceder a realizar búsquedas comparándolas con una lista de sitios maliciosos previamente descargada.

Finalmente, se realiza pruebas simulando un ataque de phishing a un usuario con la finalidad de comprobar el correcto funcionamiento del proyecto.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍAS

ACL (Access Control List) Lista de control de acceso.

CLI (Command Line Interface) Interfaz de Línea de Comandos

FTP (File Transfer Protocol) Protocolo de Transferencia de Archivos

GNU GPL (GNU General Public License) Licencia Pública General de GNU

GUI (Graphical User Interface) Interfaz Gráfica de Usuario

HTTP (Hipertext Transfer Protocol) Protocolo de Transferencia de Hipertexto

HTTPS (Hipertext Transfer Protocol Secure) Protocolo Seguro de Transferencia de Hipertexto

IDS (Intrusion Detection System) Sistema de detección de intrusos.

IP (Internet Protocol) Protocolo de internet.

IPS (Intrusion Prevention System) Sistema de prevención de intrusos.

URL (Uniform Resource Locator) Localizador de Recursos Uniforme

GLOSARIO

ANTIVIRUS.- Programa que ayuda a proteger el ordenador de malware.

ATAQUE INFORMÁTICO.- Método por el cual una o varias personas intentan causar problemas, daños o robos de información en un sistema informático.

FIREWALL.- Software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

IDS.- Programa que detecta accesos no autorizados a un computador o una red.

INDEXAR.- Ordenar datos o información de acuerdo a un criterio.

MALWARE.- Software malicioso cuyo objetivo es infiltrarse o dañar un sistema sin el conocimiento del propietario

SCRIPT.- documento que contiene instrucciones, escritas en códigos de programación

SPLUNK.- Software para buscar, monitorear y analizar datos generados por máquinas (Big Data) de aplicaciones, sistemas e infraestructura IT a través de un interfaz web.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El crecimiento de los ataques informáticos así como su complejidad ha creado la necesidad de encontrar maneras que permitan responder de manera inmediata a posibles ataques. Toda la información generada por aplicaciones, servidores, dispositivos de seguridad en las redes, etc. contienen información valiosa; la cual puede ayudar a identificar amenazas de seguridad en una organización. Un análisis manual de todos estos datos tomaría demasiado tiempo, y para cuando la organización trate de reaccionar, el atacante habrá tenido tiempo suficiente para infiltrarse dentro de la red. Analizar todos estos datos de manera automatizada es la clave para una rápida detección y respuesta ante posibles ataques informáticos.

Splunk provee una solución a este problema. Splunk puede recibir todo tipo de información generada por distintos dispositivos, de tal manera que un administrador puede investigar incidentes de seguridad en minutos permitiéndole responder a un posible ataque casi inmediatamente.

CAPÍTULO 1

GENERALIDADES

1.1 Descripción del problema

Los datos generados por los distintos sistemas y dispositivos de una infraestructura tecnológica, contienen información valiosa sobre las actividades del negocio, el comportamiento de los dispositivos, amenazas de seguridad, entre otros. El rápido crecimiento de esta información, así como su complejidad convierten el análisis de esta información en una tarea ardua y que requiere demasiado tiempo.

En la actualidad, los criminales informáticos están constantemente tratando de encontrar vulnerabilidades y fallas de seguridad dentro

de las organizaciones con el fin de explotarlas . Los usuarios son la vulnerabilidad más grande que posee una organización, es por esta razón que existen muchos sitios maliciosos en Internet. Gran parte de los ataques informáticos se originan de las visitas a sitios maliciosos por parte de usuarios inexpertos.

El acceso a sitios maliciosos compromete la seguridad de la información y de la red, ya que el fin de estos sitios es efectuar alguna actividad maliciosa sobre el equipo o red de quien los visita.

En el instante en que un evento de seguridad ocurre en la organización, el analista de seguridad debe identificar que está sucediendo, quien está atacando y como lo está haciendo; con el fin de contener el ataque en el menor tiempo posible.

Los sistemas de seguridad como antivirus, firewalls, web proxies, IDS, etc. ayudan a detectar y responder a eventos de seguridad pero no siempre son suficiente y más aún cuando trabajan de manera independiente. Toda la información generada por aplicaciones, servidores, la red, dispositivos de seguridad, etc. proporcionan información relevante al momento de identificar un ataque de

seguridad.

El análisis manual de toda esta información requiere demasiado tiempo; favoreciendo así al atacante, ya que para cuando la organización tenga un indicio de lo que está sucediendo y trate de reaccionar; el atacante ya ha tenido suficiente tiempo para infiltrarse dentro de la red y afectar la continuidad del negocio. Analizar la información de una manera eficaz es la clave para detectar, responder y contener los ataques de seguridad.

1.2 Solución propuesta

La información es el principal activo de una organización, teniendo como objetivo primordial garantizar su confidencialidad, disponibilidad e integridad.

Cualquier ataque de seguridad hacia la organización que no pueda ser contenido y mitigado de manera inmediata tendrá grandes repercusiones sobre el negocio, ya que afectará la productividad causando pérdidas monetarias y además, afectará la imagen de la organización.

Este proyecto está orientado a la implementación de una plataforma

que permita integrar toda la información generada por los distintos dispositivos de la red en un solo lugar con el fin de prevenir ataques de seguridad. Para ello, se hará uso de SPLUNK, el cual es un software de agregación de datos que permite recolectar e indexar la información generada por cualquier dispositivo en tiempo real.

SPLUNK agregará toda la información correspondiente a eventos de seguridad desde cualquier fuente a un solo sistema, lo que nos ayudará a eliminar el problema de tener que analizar la información en los distintos sistemas de seguridad para encontrar una amenaza.

Esta solución propone específicamente crear una plataforma que permita la detección automatizada de accesos a sitios maliciosos, generando alertas que serán disparadas cuando cualquier usuario de la organización visite URLs que se encuentren en el listado de sitios maliciosos. Estas alertas serán enviadas automáticamente por email a los analistas de seguridad e incluirán IP y nombre del equipo posiblemente infectado, permitiendo a los analistas tomar acciones remediales.

Gracias a la implementación de la solución se podrá conocer si

alguien visita un sitio malicioso en el momento exacto en el que está ocurriendo, lo cual permitirá prevenir futuros daños en la red.

La implementación del proyecto se basa en el análisis de todos logs generados por servidores proxy, el mismo que se encarga de controlar el acceso a internet de todos los usuarios de una organización. Splunk es el encargado de importar todos estos logs y realizar la comparación de los accesos de los usuarios con una lista de dominios maliciosos previamente definida y actualizada diariamente (PHISTANK WATCHLIST). Si un usuario accede a un dominio de la lista definida, una alerta que contiene la ip del usuario afectado, el sitio al que trata de acceder y el tiempo en el que se disparo alerta, es enviada al analista de seguridad.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Logs

Un log es un registro de eventos ocurridos dentro de los sistemas y redes de la organización. Los cuales están compuestos por entradas, donde cada entrada contiene información relevante a un evento específico que ha ocurrido dentro de la red. Los logs poseen varias utilidades como: optimizar un sistema, mejorar el rendimiento de la red, llevar un registro de las acciones de los usuarios, proveer información útil para investigar actividades maliciosas, etc [1]. Este

proyecto se enfoca principalmente en los logs creados por los servidores proxies.

2.1.1 Logs de Seguridad

Los logs contienen información relacionada a diferentes tipos de eventos que ocurren dentro la red de una organización. Muchos logs contienen información relacionada a la seguridad de la información. Sistemas de seguridad comunes incluyen lo siguiente:

- Antivirus: registra todas las instancias de los programas maliciosos detectados, intentos de desinfección de archivos y archivos en cuarentena.

- Corta Fuegos: Permiten o bloquean actividades de acuerdo a políticas previamente establecidas. Los corta fuegos pueden llevar un registro del estado del tráfico en la red y realizar análisis de contenido. Los Corta fuegos crean registros para todas estas actividades.

- Web Proxies: Mantienen registros de todas las URLs accedidas a través de él.

- Sistemas de Detección y Prevención de intrusos: registran información detallada sobre comportamiento sospechoso y ataques detectados, así como también acciones preventivas ejecutadas para detener actividades maliciosas en progreso. [1]

2.2 Splunk

Splunk es un programa de agregación de datos que permite la recolección y el indexamiento de los datos generados por dispositivos tecnológicos desde cualquier fuente o ubicación en tiempo real. Una organización puede usar Splunk para recopilar toda la información relacionada a seguridad desde cualquier fuente como logs de antivirus, corta fuegos, proxies, sistemas IDS, etc. en un solo sistema. Esto evita el problema de tener que buscar información dentro de los distintos sistemas de seguridad para poder encontrar una amenaza.

Información desde equipos remotos pueden ser capturados gracias al módulo de reenvío de datos que provee Splunk. Una vez que la información es recolectada, los administradores pueden realizar análisis a través de búsquedas, reportes u operaciones de diagnóstico utilizando la interfaz web del software. Splunk puede

también enviar alertas (email, correr un script, etc.) basadas en criterios previamente configurados. Splunk provee una imagen completa de toda las infraestructura de la organización permitiendo una rápida respuesta a posibles ataques.

2.3 Infraestructura Splunk

Splunk tiene soporte para diferentes plataformas tales como Windows, Linux, Solaris, entre otros. El esquema más sencillo es el por default: indexamiento y búsquedas en el mismo servidor. Dependiendo de la infraestructura de la organización, componentes de Splunk como los forwarders pueden ser instalados en los distintos servidores para enviar datos al servidor indexador.

Los datos recopilados por Splunk pueden ser accedidos desde la interfaz Web de Splunk o el CLI, permitiéndole al usuario monitorear, hacer búsquedas y crear reportes.

Esta sección introduce de manera general algunos componentes y características de Splunk.

2.3.1 Indexer

Un indexer es la instancia de Splunk encargada de indexar datos. Los indexadores transforman datos sin procesar en eventos y los almacena dentro de un índice. El indexador también permite realizar búsquedas sobre la información indexada. [2]

2.3.2 Forwarder

Un forwarder es una instancia de Splunk que reenvía datos a otra instancia de Splunk (a un indexer o a otro forwarder) o a otra clase de sistemas. [2]

2.3.3 Interfaz Web de Splunk – GUI

Splunk Web permite al usuario configurar datos de entrada, búsquedas sobre la información, visualizar resultados e investigar eventos de seguridad. Splunk Home incluye la barra de navegación, el panel de aplicaciones, el panel de exploración y un área de trabajo personalizable.

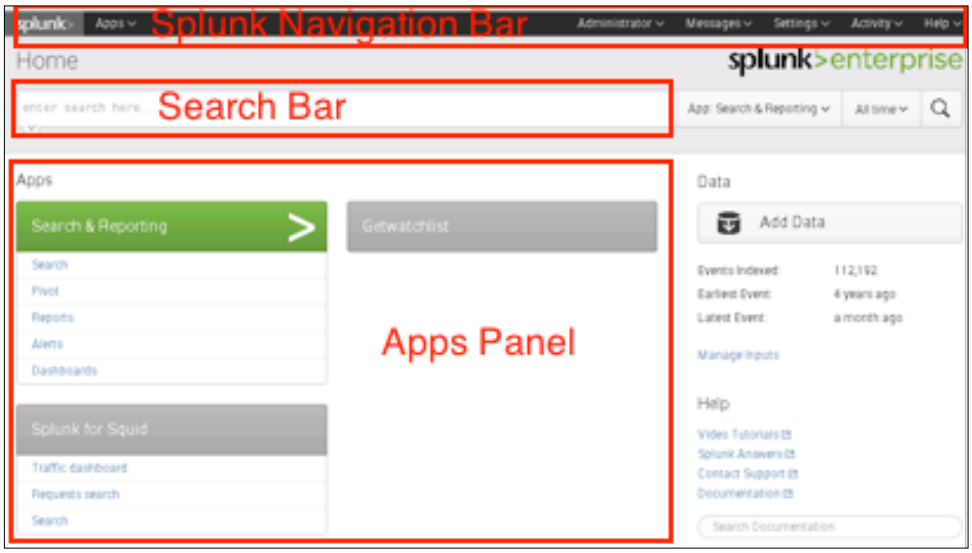


Figura 2.1: Interfaz Web de Splunk

2.3.4 Búsquedas (Queries)

La barra de búsqueda es la principal manera de navegar sobre los datos en Splunk. El usuario puede escribir búsquedas sobre eventos de un índice, usar comandos estadísticos para calcular métricas o generar reportes, realizar búsquedas con condiciones especiales e identificar patrones.

Para acceder a las búsquedas desde Splunk home, debe dar click en **Search & Reporting** en **Apps.** La figura 2.2 muestra los principales componentes de la aplicación de búsquedas:

- **App barra:** Permite al usuario navegar entre los diferentes Menús que provee la aplicación Search & Reporting.

- **Barra de Búsqueda (Search bar):** Corre las búsquedas en Splunk.

- **Selector de tiempo (Time range picker):** Retorna los eventos en un periodo de tiempo especificado. El rango de tiempo tiene rangos pre configurados o el usuario puede personalizar el rango de tiempo.

- **Cómo Buscar (How to search):** Link al tutorial y manual de búsquedas para aprender a escribir búsquedas.

- **Qué Buscar (What to search):** Muestra un resumen de los datos recolectados por Splunk.

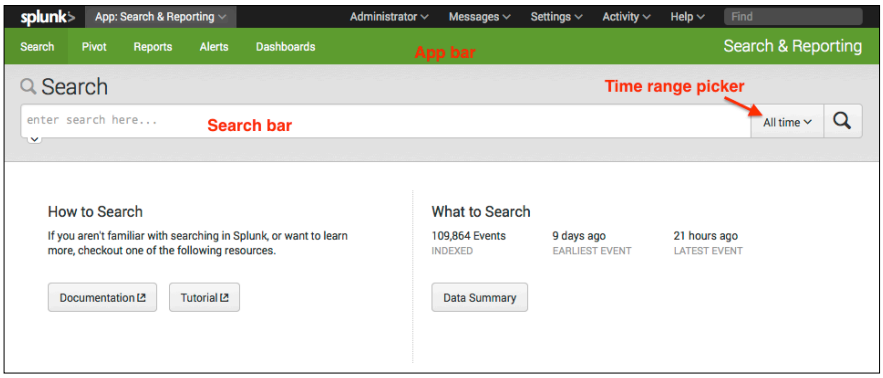


Figura 2.2: Interfaz de Búsqueda [3]

Para hacer búsquedas, un query puede ser escrito en la barra de búsqueda. Una vez que el query es insertado una página de resultados se abrirá . Esta página mantiene la barra de búsqueda y el selector de rango de tiempo pero muestra otros elementos como:

• **Línea de Tiempo (Timeline):** Es una representación visual del numero de eventos obtenidos en un periodo de tiempo especifico.

• **Barra de campos (Fields sidebar):** Cuando Splunk indexa datos, automáticamente reconoce y extrae los campos relevantes de esos datos. Estos campos son mostrados cuando una búsqueda es ejecutada.

• **Lista de Eventos (Event List):** Muestra los eventos que coinciden con las búsquedas.

• **Menú Guardar (Save as menu):** Provee opciones de guardar los resultados de las búsquedas como reporte, panel en el área de trabajo o tipos de eventos. [3]

La Figura 2.3 muestra los principales componentes de la página de resultados de búsqueda:

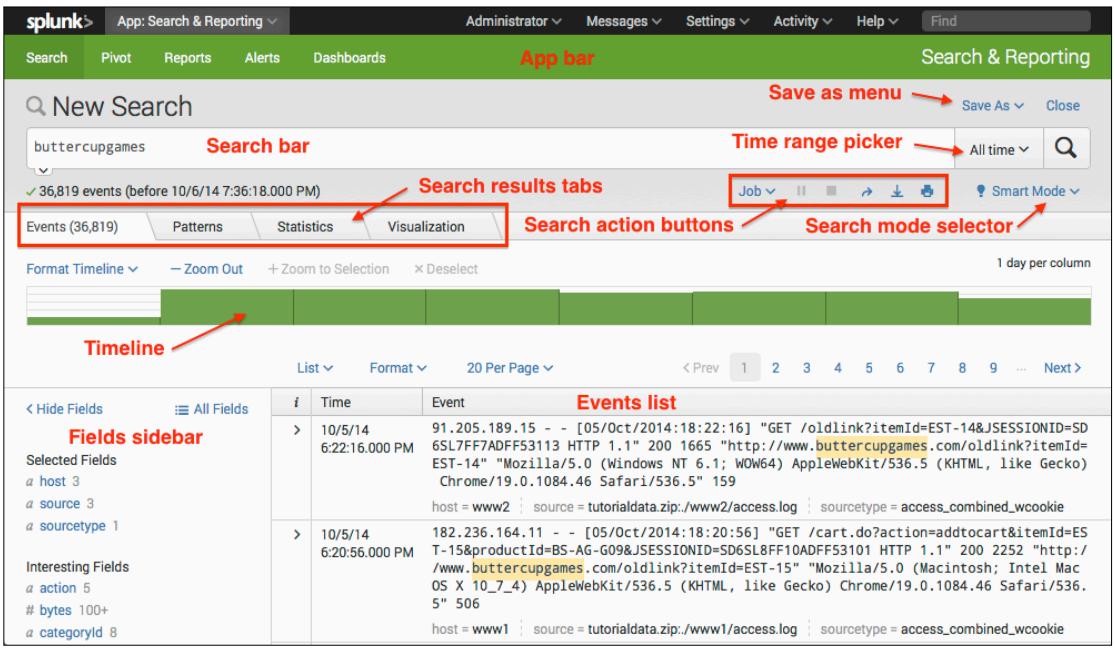


Figura 2.3: Resultados de Búsqueda [3]

Ejemplo 1: Escribir el query **index=squid** en la barra de búsqueda.

Esta búsqueda devuelve todos los eventos que coinciden con el string squid. Cada evento provee información relevante que Splunk ha indexado por sí mismo, tales como: nombre del host, IP origen, Estado del requerimiento http y la URL.

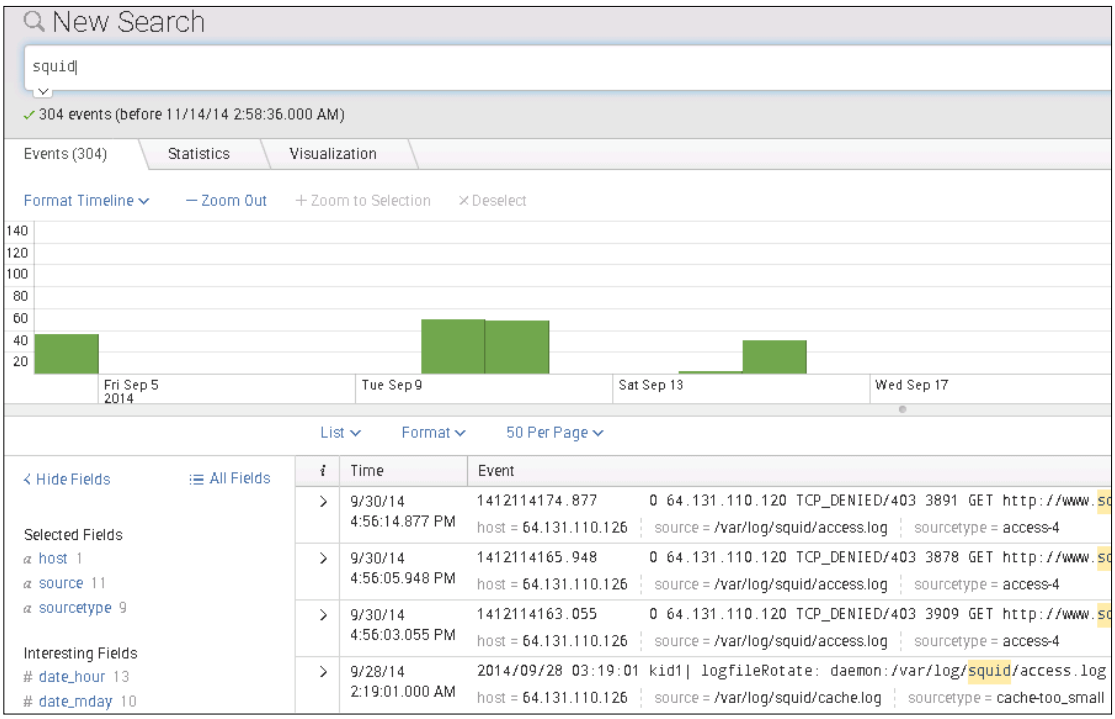


Figura 2.4: Resultados para el query “squid”

Ejemplo 2: Ejecute el query http://www.baidu.com.

Esta búsqueda mostrará todos los equipos que han visitado este sitio web. Si el sitio web es un dominio malicioso, este simple query proveerá suficiente información al administrador para detectar posibles infecciones en los sistemas en pocos segundos.

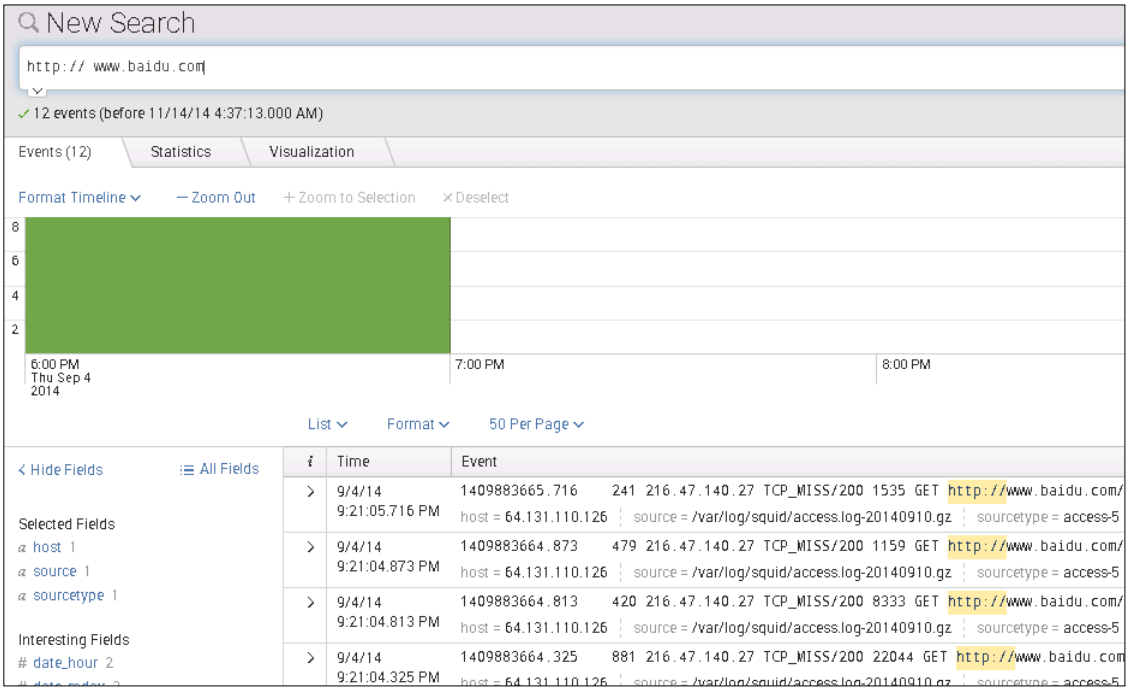


Figura 2.5: Resultados para el query "http://www.baidu.com"

Una búsqueda manual que consiga la misma tarea podría tomar demasiado tiempo. Este proyecto buscar automatizar estas búsquedas tediosas y proveer alertas en tiempo real.

2.3.5 Alertas

Las alertas pueden ser configuradas para dispararse cuando una acción cumpla ciertas condiciones previamente configuradas en las búsquedas. Las alertas ejecutan acciones como enviar información a correos electrónicos, publicar información de alertas en fuentes RSS, etc.

2.3.6 Splunk Aplicaciones

Las aplicaciones son agrupaciones de configuraciones, objetos y vistas personalizadas que extienden el ambiente de Splunk para cumplir con necesidades especificas de diferentes usuarios. Una instalación de Splunk puede correr múltiples aplicaciones simultáneamente. [2]

Squid App and Getwatchlist app para Splunk son requeridas para desarrollar este proyecto.

Squid App para Splunk

Squid app detecta campos específicos de los logs de acceso de Squid, tales como: ip del cliente, http_status, IP del servidor, entre otros. Squid app facilita las búsquedas al administrador y provee un área de trabajo personalizable que muestra información importante como las direcciones IPs más visitadas por los usuarios, la IPs de los clientes que más accesos realizan, etc. Un administrador puede personalizar esta área de trabajo con búsquedas de su interés.

La siguiente figura muestra los sitios webs más visitados por los usuarios (características disponible en el área de trabajo de Squid).

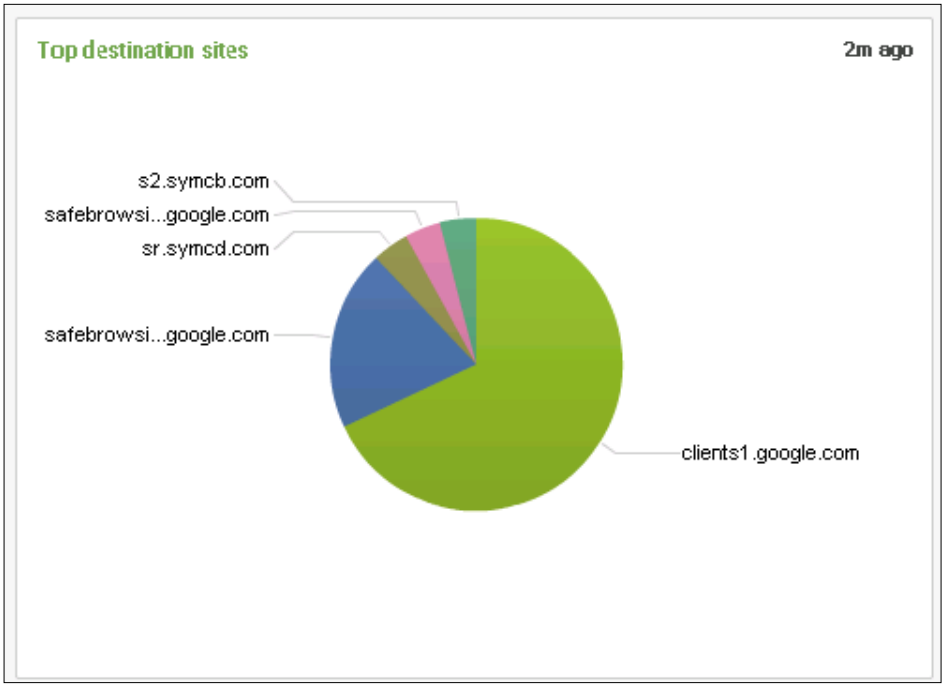


Figura 2.6: Squid app para Splunk

Squid App solamente trabaja con tipos de archivos generados por el servicio Squid, por lo que es necesario configurar el tipo de fuente (sourcetype) a "squid" en el archivo inputs.conf en el servidor proxy dentro del componente forwarder.

Getwatchlist app para Splunk

Getwatchlist app proporciona comandos especiales de búsqueda para Splunk, los mismos que permiten descargar listas de sitios maliciosos desde internet y almacenarlos en archivos CSV. Esta funcionalidad es útil para crear tablas de búsquedas tanto desde fuentes internas como externas y mantenerlas actualizadas a la fecha. Estas listas pueden contener cualquier dato, como por ejemplo: nombres de dominios, nombres de equipos, direcciones de correo, nombres de archivos, etc., los mismos que pueden ser usados en búsquedas sobre eventos indexados.[4]

La aplicación Getwachlist está disponible en: http://splunk-base.splunk.com/apps/24216/getwatchlist

2.4 Web Proxy

Un Web Proxy controla los accesos de los usuarios a Internet de acuerdo a reglas previamente establecidas por el administrador, añadiendo una capa más de protección entre los clientes Web y los servidores Web. Los Web proxies también copian en cache paginas web accedidas para hacer el acceso a estas páginas más eficiente.

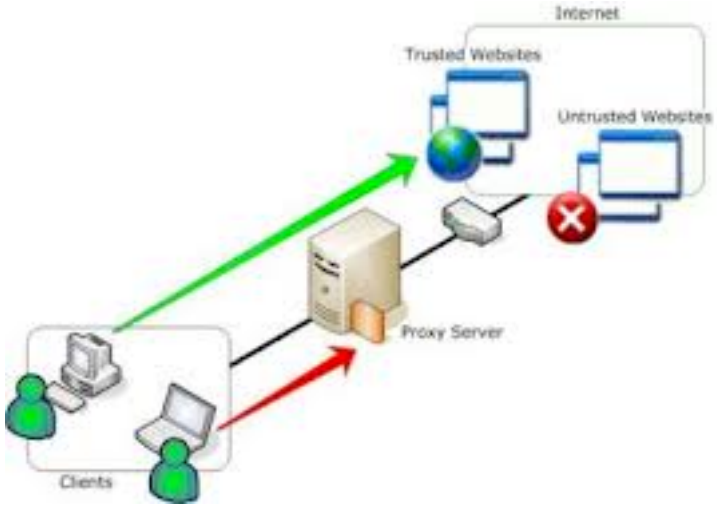


Figura 2.7: Esquema Web Proxy

Cuando un Web proxy recibe un requerimiento de una página, el proxy busca en su cache local; si la página existe, la devolverá al usuario sin necesidad de reenviar el requerimiento al Internet. Si la página no está en cache, el servidor proxy actúa como un cliente y solicita la página web al servidor en Internet; cuando la página es devuelta, el servidor proxy la reenvía al usuario.

Un servidor proxy es utilizado para incrementar la seguridad de la red. Los servidores web proxy generan información relevante para análisis de seguridad, esta información es almacenada en logs.

Los logs registran información de accesos, errores de configuración y

consumo de recursos. Existen varios logs generados por los servidores proxy pero para análisis de seguridad, las entradas más importantes son las de acceso contenidas en el archivo **access**.log

El servicio de Squid Proxy es usado para implementar el servidor proxy en la infraestructura del proyecto.

2.4.1 Squid

Squid es un servidor proxy para la Web que soporta HTTP, HTTPS, FTP, etc. Squid ayuda a reducir el consumo de ancho de banda y mejorar los tiempos de respuestas, almacenando en cache páginas web accedidas frecuentemente. Además, provee una amplia gama de controles de acceso, así como también convierte al servidor en un acelerador de requerimientos.

Squid está disponible para la mayoría de sistemas operativos, incluyendo Windows y está bajo la licencia GNU GPL [5]. Squid es el servidor proxy más popular para los sistemas Unix/Linux.

Squid crea 3 logs principales: store.log, cache.log and access.log. Access.log es el más relevante para el propósito

del proyecto ya que contiene la IP del cliente, la IP de destino, el tiempo (timestamp), la URL de destino, entre otros; información necesaria para la ejecución del proyecto. Sin embargo, cuando un cliente accede a una página web se crean logs no solamente para el sitio principal sino también, para avisos publicitarios u otras partes del sitio. Comúnmente un sitio web contiene docenas de links asociados, los mismo que serán registrados por el servidor proxy.

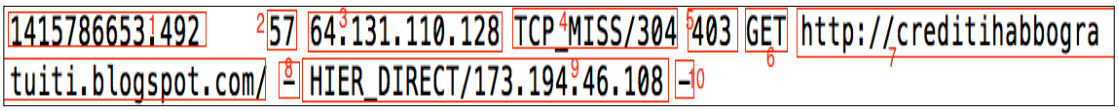


Figura 2.8: Ejemplo de registro en el archivo access.log

La figura 2.8 muestra un ejemplo de una entrada en el archivo access.log.

Tabla 1: Campos de las entradas del archivo access.log [6]

Campo	Nombre del campo	Descripción
1	Tiempo (Timestamp)	Tiempo del requerimiento del cliente en segundos.
2	Elapsed	Tiempo que el servidor de tráfico destina al procesamiento del requerimiento del cliente en milisegundos.
3	Equipo Remoto	Direcion IP del cliente
4	Código/estado	Como la cache responde al requerimiento.

5	Bytes	Tamaño de la respuesta al cliente en bytes.
6	Método	Método del Requerimiento Request Method.
7	URL	URL solicitada por el cliente.
8	Rfc931	Username del cliente autenticado.
9	Peerstatus/ Peerhost	Servidor de tráfico usado para obtener los objetos.
10	Tipo	Tipo de Contenido de la respuesta del Proxy.

La Tabla 1 muestra el significado de cada campo de las entradas en un log. En la Figura 2.8, el usuario con IP 64.131.110.128 accedió a la URL htttp://creditihabbogratuiti.blogspot.com, la cual tiene la dirección IP: 173.194.46.108. Esta entrada, permite identificar que un usuario en especifico visitó un sitio malicioso y posiblemente se haya infectado.

Access.log tiene millones de entradas por día. Splunk indexa y procesa todas estas entradas, haciendo posible crear alertas que se disparen en tiempo real.

2.5 Dominios Maliciosos / Watchlists

Algunas organizaciones mantienen y publican listados de direcciones IPs y URLs de sistemas y redes sospechosas de realizar actividades maliciosas. Estas listas pueden ser usadas para

monitorear actividades en la red y configurar alertas en contra de ellas. Algunas de las listas disponibles son:

http://www.malwaredomainlist.com/mdl.php

http://mirror1.malwaredomains.com/files/domains.txt

http://www.abuse.ch/zeustracker/blocklist.php?download=ipblocklist

Cuál usar? Esto dependerá de las necesidades específicas de cada organización. Más de una lista puede ser usada con el fin de obtener una base de datos más completa. Sin embargo, para propósitos demostrativos solo se usará la lista de sitios maliciosos de PhishTank ya que en el proyecto se simulará un ataque de phishing.

2.6 Ataque Phishing

Phishing es un ataque común que sigue creciendo día a día. Es el acto de adquirir información sensible como usuarios, contraseñas, números de tarjetas de crédito, etc. suplantando una compañía legítima en una comunicación electrónica. Los criminales cibernéticos realizan este ataque instalando programas maliciosos en la computadora de la victima o robando información personal de la computadora de la víctima o re direccionando a la víctima a un sitio

erróneo.

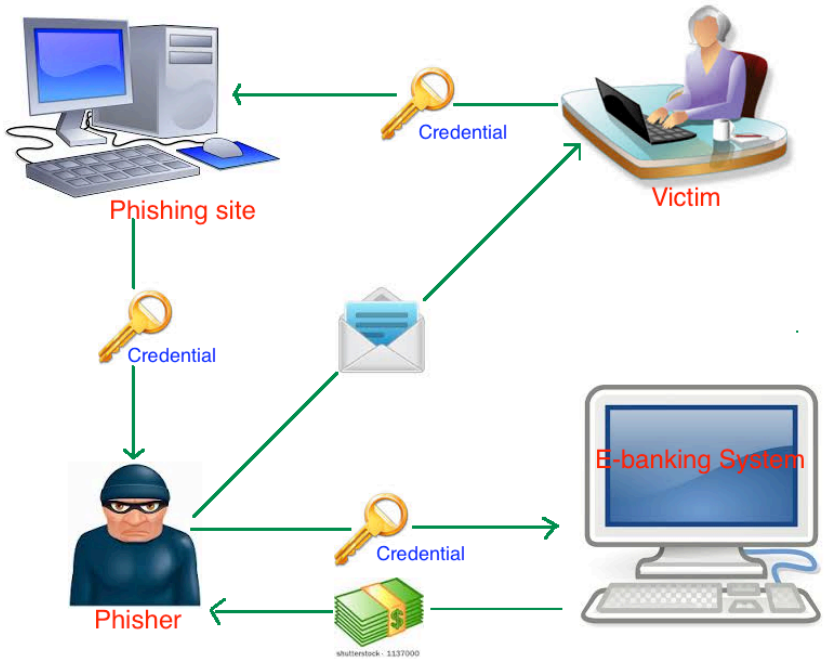


Figura 2.9: Esquema de un ataque de Phishing por correo electrónico

Phishing es usualmente llevado a cabo usando correos electrónicos. El atacante envía correos de phishing a las víctimas. El correo de Phishing re direcciona al usuario a visitar un sitio web donde el atacante solicita actualizar información personal. La Figurea 2.9 muestra un esquema de ataque de phishing por email.

Hackers comúnmente usan redes sociales como Facebook, Twitter, Myspace etc., para atacar a las víctimas.

2.7 PhishTank Watchlist

PhishTank es un sitio colaborativo para información sobre phishing en Internet. También, PhishTank provee un API libre para desarrolladores e investigadores para integrar datos anti phishing en sus aplicaciones sin cargo. [7]

PhishTank Watchlist ayudará a crear alertas cuando los usuarios visiten un sitio malicioso. PhishTank watchlist está disponible en http://data.phishtank.com/data/online-valid.csv y los datos están en múltiples formatos y son actualizados cada hora..

Para descargar estos archivos de manera automática es necesario registrarse en la página http://www.phishtank.com/login_required.php para recibir una clave. Sin la clave, existe una limitación del número de descargas por horas que se pueden realizar.

Usando la clave, la watchlist debe ser descargada de la URL de esta manera:

```
http://data.phishtank.com/data/<your app key>/online-valid.json.bz2
```

CAPÍTULO 3

IMPLEMENTACIÓN

3.1 Ambiente de Prueba

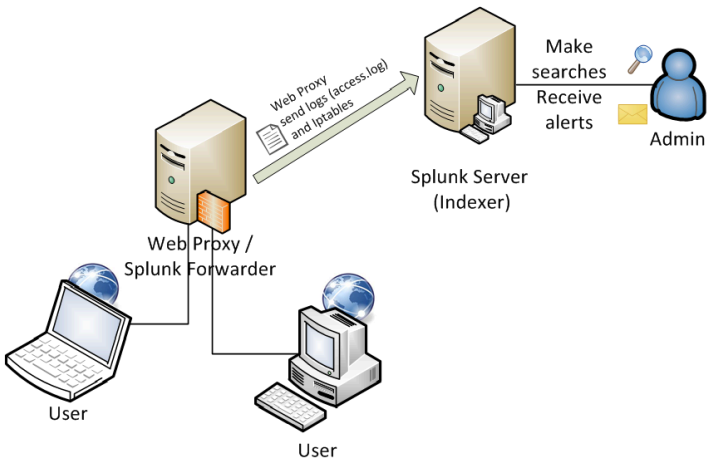


Figura 3.1: Ambiente del Proyecto

Para conseguir los objetivos del proyecto es necesario configurar dos

servidores y una estación de trabajo (equipo del usuario). Los servidores pueden ser construidos en hardware o de manera virtual dependiendo de los recursos de la organización. La Figura 3.1 muestra que el servidor Web Proxy actúa como un gateway permitiendo o denegando el acceso a Internet a los usuarios, además tiene instalado el componente de Splunk forwarder para enviar los logs de acceso al servidor principal Splunk. El servidor Splunk (indexer) colecta y procesa todos los logs enviados desde el servidor proxy y provee la interfaz donde el administrador puede realizar búsquedas, crear reportes o configurar alertas sobre los datos indexados.

El servidor Splunk fue configurado en Windows Server 2012 (64 bit), en donde se instaló la versión Enterprise de Splunk y se configuró una licencia de desarrollador. La licencia de desarrollador incluye características necesarias para el proyecto como los mensajes de alertas. Splunk está disponible en http://www.splunk.com/download/ donde puede ser descargado gratis con una licencia de prueba de 60 días. Squid y GetWatchlist Apps para Splunk fueron instaladas en el servidor Indexer. Squid para

Splunk ayuda a reconocer los campos de los registros del archivo access.log. Y GetWatchlist App ayuda con las búsquedas en la información indexada, comparando la información contra datos de Fuentes externas como una lista de sitios web maliciosos.

Tabla 2: Características del Servidor Splunk

Sistema Operativo	Windows 2013 Server 64 bits
Software	Splunk Enterprise 6.1.4
Licencia	Splunk Developer Personal License NOT FOR RESALE
Dirección IP:	64.131.110.128
Splunk Apps:	GetWatchlist Splunk for Squid

El servidor Web Proxy fue instalado en Fedora 20, el cual incluye el servicio de Squid durante la instalación. El servicio de Squid usa el Puerto 3128 por default y cualquier otra configuración necesaria para este servicio se la realiza en el directorio **/var/log/squid.** El servidor proxy también necesita el componente Forwarder de Splunk para poder enviar los access.log al indexer. El forwarder es instalado bajo el directorio **/opt/splunkforwarder** y sus configuraciones pueden ser encontradas en el mismo directorio. Splunk forwarder usa el Puerto 9997 para el reenvío de datos. El servicio ssh usa el Puerto 22.

Tabla 3: Características del Servidor Web Proxy

Sistema Operativo	Fedora 20 (64 bits)
Modo gráfico	No es necesario
Servicios requeridos	Squid Iptables Splunk forwarder
Dirección IP:	64.131.110.126
Puertos importantes	3128 Web Proxy service 9997 Splunk forwarder 22 ssh (acceso remoto permitido)

La estación de trabajo del usuario puede ser cualquier dispositivo con acceso a Internet a través del servidor proxy. En este caso, una computadora personal es usada.

3.1.1 Instalación y Configuración de Squid

En el servidor proxy corriendo en Fedora 20, se deberá seguir los siguientes pasos:

1. Verificar si el servicio Squid está ya instalado en el sistema.

Abrir una consola y ejecutar el comando **rpm –q squid**.

```
[rice@localhost ~]$ rpm -q squid
squid-3.3.12-2.fc20.x86_64
```

Figura 3.2: Verificando si squid está instalado.

En este caso el servicio ya está instalado pero si no lo estuviese ejecutar **sudo yum install squid** como root e ingresar la

contraseña de root para instalarlo.

2. Iniciar el servicio squid desde el boot.

Ejecutar **sudo systemctl start squid** como root.

systemctl enable squid

En este punto el servicio ha sido instalado y configurado para que inicie apenas la máquina se encienda.

3. Editar archivos de configuración.

Squid fue instalado bajo el directorio /**etc/squid/** y cualquier configuración requerida deberá ser realizada en el archivo **/etc/squid/ squid.conf.**

El servicio Squid requiere configuraciones mínimas para funcionar. Añadir la siguiente información básica para empezar a usar el servicio web proxy en los clientes.

Ejecutar **vi /etc/squid/squid.conf** y tipiar **i** para editar.

```
acl mylan src 208.59.147.202/24     #Red que navega a través del web proxy.
http_access allow mylan             #Permite acceso a la red
http_access deny all                #Deniega accesso a otros hosts.
http_port 3128                      #Puerto en el cual squid trabaja.
```

Una vez que los cambios mencionados arriba sean realizados, presione **scape** y escriba **:wq** para guardar y cerrar el archivo.

4. Finalmente, reinicie el servicio. Ejecute **Service squid restart.**

3.1.2 Configuración de la estación de trabajo (Usuario)

Para que Internet Explorer use a web proxy, deberá seguir las siguientes instrucciones.

1. Abrir el navegador Internet Explorer Web

2. En el menú **Tools**, click **Internet Options**, click en la pestaña **Connections**, y luego click **LAN Settings**.

3. En **Proxy server**, seleccione **Use a proxy server for your LAN** .

4. En el campo **Address**, escriba la dirección IP del servidor proxy: **64.131.110.126**

5. En el **Port** , escriba el Puerto usado por el servidor proxy para escuchar a sus clientes: **3128**

6. Click **OK** para cerrar la pestaña **LAN Settings**.

7. Click **OK** para cerrar la ventana de diálogo de **Internet Options**.

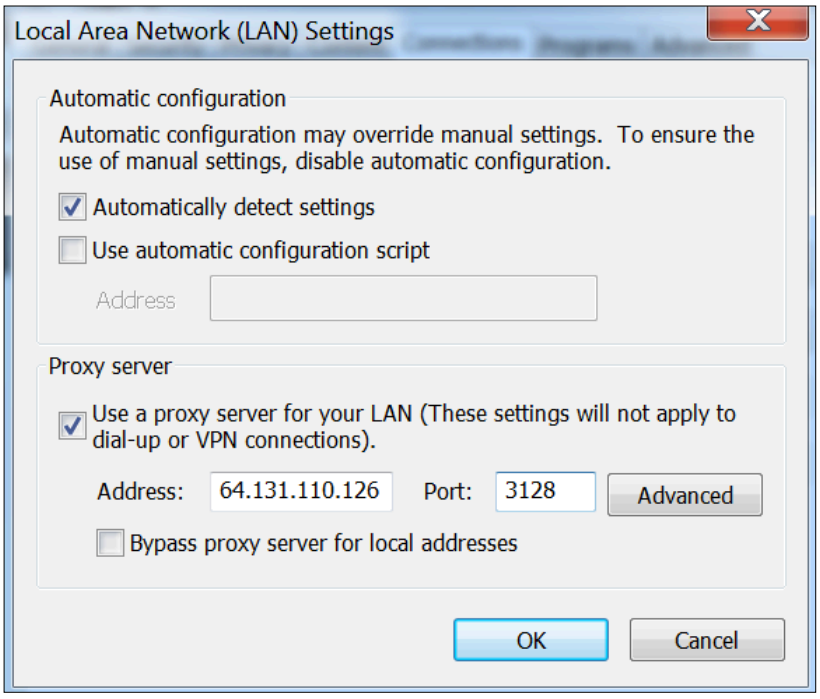


Figura 3.3: Internet Explorer – configuración Web Proxy.

Una vez el servidor proxy esté configurado en el navegador, el usuario deberá tratar de navegar en Internet para verificar que el proxy esté funcionando. Si el proxy está funcionando, la página solicitada debería ser presentada.

3.1.3 Instalación Splunk Indexer

Seguir los siguientes pasos para instalar Splunk Enterprise en Windows.

1. Descargar el instalador desde http://www.splunk.com/download/. (Escoja el instalador de acuerdo a la arquitectura del sistema operativo instalado en la máquina)

2. Doble click en el archivo instalador.

3. En el panel de bienvenida, click Next.

4. Lea el acuerdo de licencia y seleccione “Check this box to accept the License Agreement" y dé click Customize Options.

5. En el panel de carpeta de destino, click Change... para especificar una ubicación o click Next para aceptar la ubicación por default. Splunk Enterprise es instalado por default en el directorio \Program Files\Splunk\ .

6. En el panel de Logon Information, seleccione Local system

user y dé click Next.

7. Seleccione Create Start Menu Shortcut y continúe.

8. Una vez instalado seleccione Launch browser with Splunk y click finish.

9. Ingrese al sistema con el usuario por default: admin y contraseña: changeme.

10. Otra ventana aparecerá preguntando cambiar la contraseña. Es recomendable cambiar la contraseña por default.

11. Una vez hecho el login, aparecerá la página principal de Splunk y estará listo para empezar a trabajar.

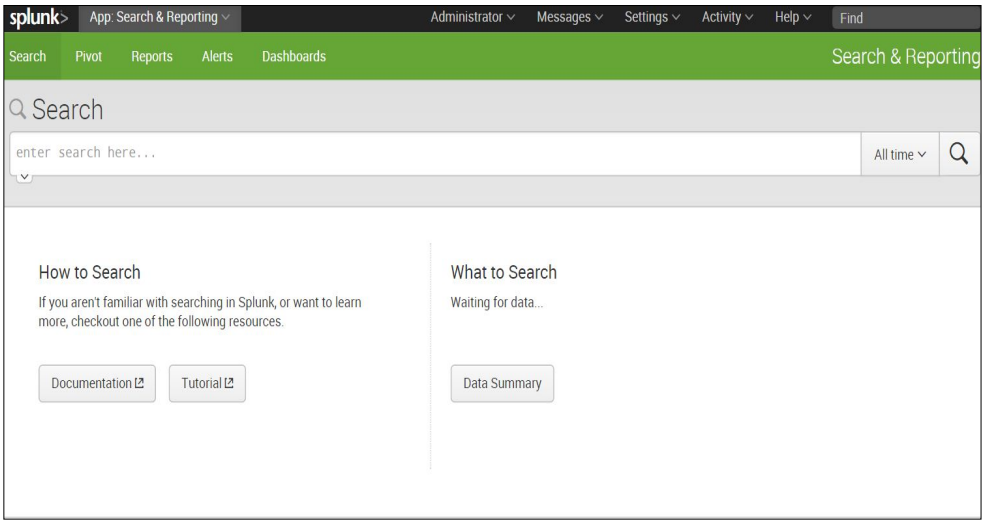


Figura 3.4: Interfaz Web principal de Splunk

3.2 Importando Datos al servidor Splunk

Con la infraestructura lista, se debe proceder a obtener la información de los logs del servidor proxy en Splunk indexer. El archivo acces.log de Squid es el que contiene los datos de nuestro interés; la manera más simple de enviar estos datos a Splunk es mediante el componente forwarder de Splunk, el mismo que reenvía los logs especificados al indexer en un formato entendible para Splunk.

El Servidor Splunk recibe los datos del servidor Proxy los almacena y los indexa. Un índice es un repositorio para datos de Splunk. Los datos recibidos son transformados en eventos y estos son asociados a un índice. Splunk asocia todos los datos en el índice principal si no se le indica otro índice. El índice **Squid_access** fue creado para asociar todos los datos provenientes del servidor squid. Este índice ayudará a organizar la información entrante y facilitar su eliminación en caso de ser necesario.

Splunk Indexer escucha los datos entrantes a través del Puerto 9997. Una simple búsqueda del query “squid” mostrará toda la información recibida desde el servidor proxy. La Figura 3.5 muestra que el indexer Splunk está recibiendo datos desde el servidor proxy.

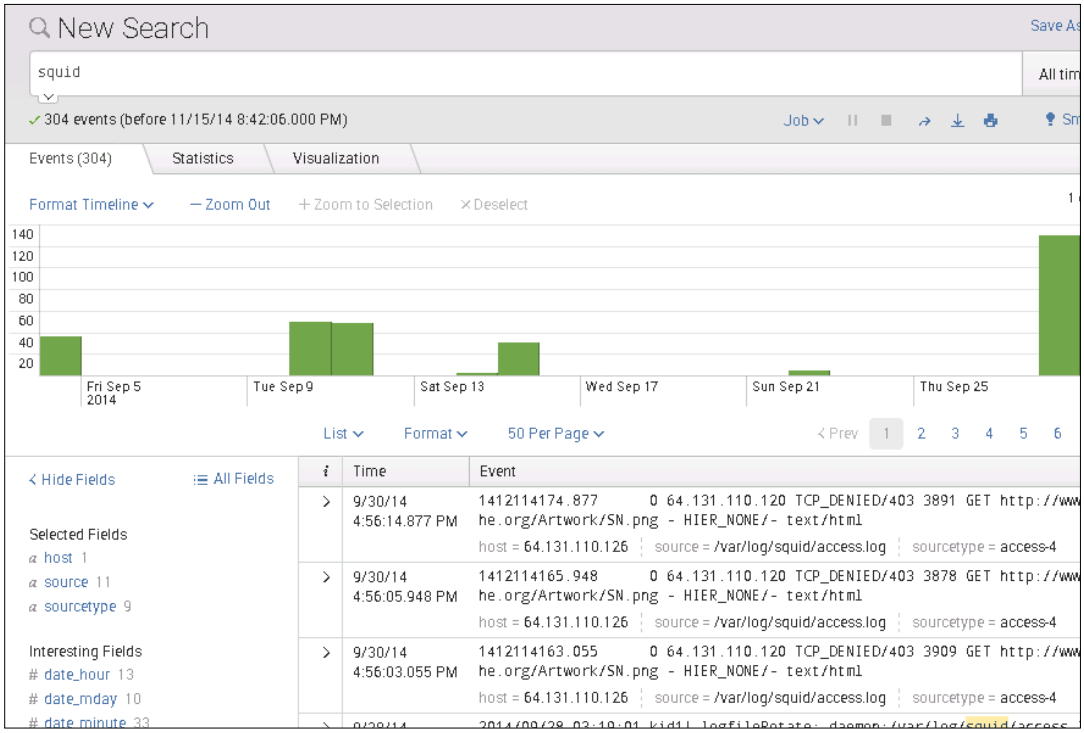


Figura 3.5: Datos recibidos desde el servidor Web Proxy.

3.2.1 Configuración del Indexer

En el servidor Splunk realice las siguientes configuraciones:

1. En el Firewall del servidor indexer, añada una nueva regla que permita recibir paquetes en el puerto 9997 desde la dirección IP del forwarder.

1.1. Abrir el Firewall de Windows, seleccione **Inbound Rules** y dé click en **New Rule**.

1.2. En **Rule Type,** seleccione **Port** y luego Next.

1.3. En **Protocol and Ports**, seleccione **TCP y Specific local ports: 9997** y click en **Next**.

1.4. En **Action**, seleccione **Allow the connection** y click en **Next**.

1.5. En **Profile**, deje las 3 opciones seleccionadas y click en **Next**.

1.6. En **Name**, especifique un nombre para la regla: **Squid for Splunk port**

2. Ingrese a la interfaz Web de Splunk con credenciales de administrador.

3. Configure el servidor Splunk (indexer) para recibir datos.

3.1. Ir a menú **Setting -> Data -> Forwarding and receiving**

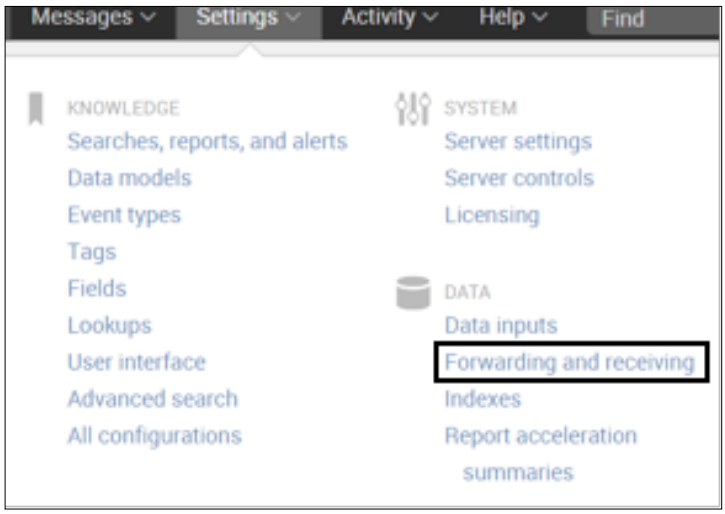


Figura 3.6: Paso 3.1

3.2. Ir al menú **Receive data -> Configure receiving –> Add new**

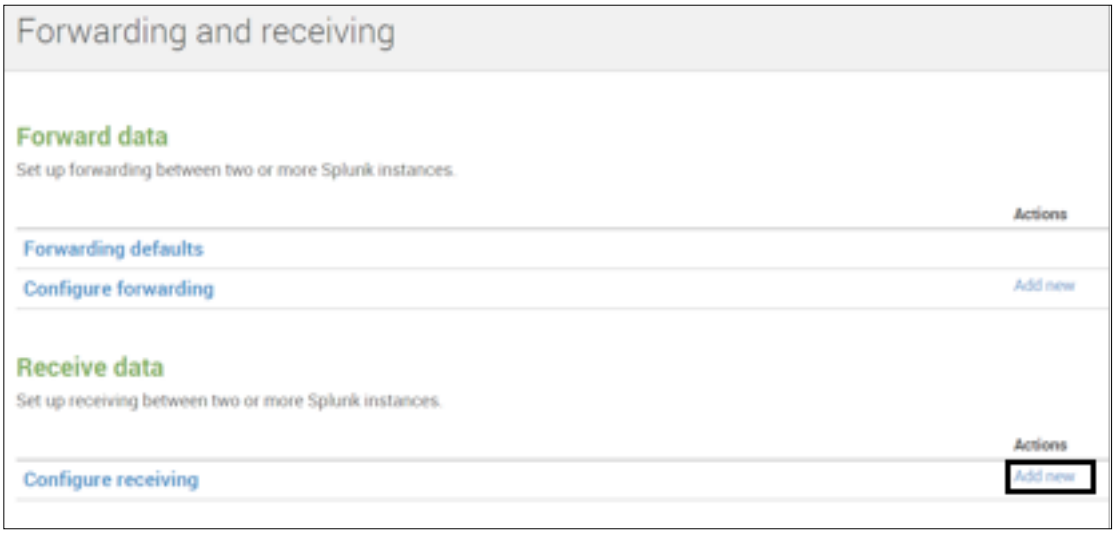


Figura 3.7: Paso 3.2

3.3. En **Listen on this port**: escriba **9997** y click en **Save.**

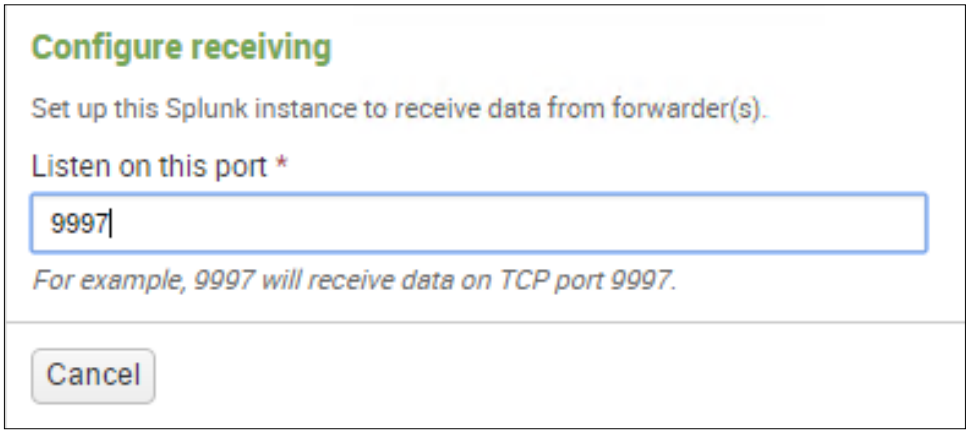


Figure 3.8: Paso 3.3

4. Instalar la aplicación Squid para Splunk.

    4.1. Descargar Squid para Splunk desde https://apps.splunk.com/app/453/

    4.2. Ir a **Apps ->Manage Apps**

    4.3. Seleccionar **Install App from file** -> Escoger el archivo descargado y click en **Upload**

5. Crear índice Squid_access.

    5.1. Ir al menú **Setting –> Data -> Indexes**

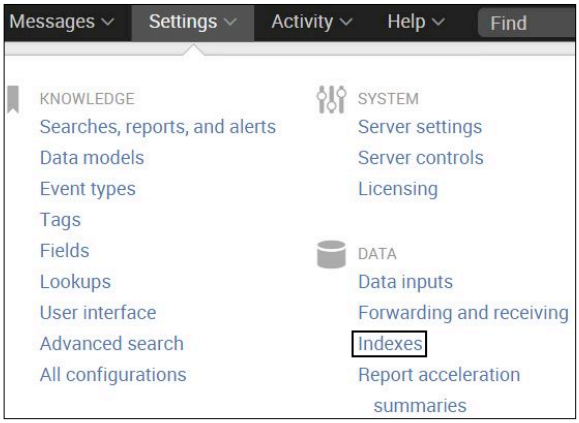


Figura 3.9: Paso 5.1

5.2. Click **New** y especificar el nombre del índice **"Squid_access"**, el resto de opciones pueden ser configuradas por default y click en **Save**.

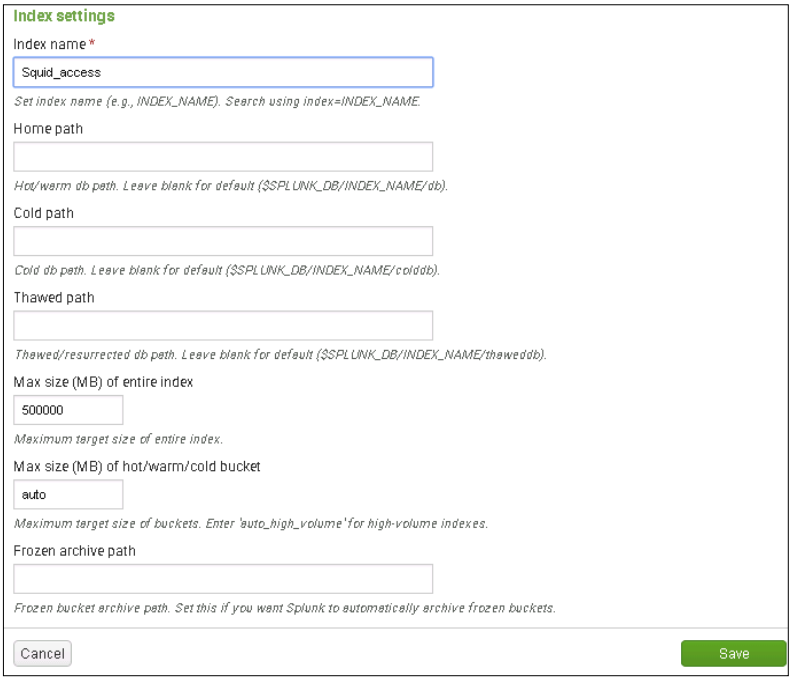


Figura 3.10: Paso 5.2

3.2.2 Configuración del componente Forwarder en Linux

En el servidor Web Proxy siga las siguientes instrucciones:

1. Descargar Splunk Universal forwarder de:

   http://www.splunk.com/download/universalforwarder. (rpm package for linux 64 bits).

2. Abrir una línea de comandos como root e instalar el Forwarder.

   Ejecutar **yum -y localinstall**

   splunkforwarder-6.2.0-237341-linux-2.6-x86_64.rpm

   El forwarder se instala en el directorio /opt/splunkforwarder/.

3. Iniciar Splunk forwarder.

   Ejecutar **cd /opt/splunkforwarder/bin**

   ./splunk start --accept-license

4. Configurar que el splunk forwarder se inicie durante el booteo.

Ejecutar **./ splunk enable boot start**

5. Configurar la conexión del Forwarder con el servidor Index

   Ejecutar **./splunk add forward-server 64.131.110.128:9997 -auth admin:changeme**

   Donde 64.131.110.128 (dirección IP del servidor Splunk):9997 (Puerto en el que recibe datos el indexer) -auth admin:changeme (contraseñas por default del forwarder).

6. Añadir los datos a reenviar.

   Ejecutar **./splunk add monitor /var/log/squid/access.log**

7. Configurar los datos a ser enviados al servidor indexer.

   Añadir la siguiente información en el archivo **inputs.conf** ubicado en **/opt/splunkforwarder/etc/system/local/**

   Ejecutar **vi /opt/splunkforwarder/etc/system/local/inputs.conf**, escribir **i** para editar y añadir los campos descritos abajo, presione

scape y escriba **:wq** para guardar y salir del archivo.

```
[monitor:///var/log/squid/access.log]        #enviar el archivo access.log
index=squid_access                           #asociar los datos al índice squid_access
sourcetype=squid                             #especificar el tipo de datos enviados al
indexer indexereindexer
```

8. Probar la conexión en el Forwarder

Ejecutar **./splunk list forward-server**

La Figura 3.11 muestra que la conexión con el indexer está activa.

```
[root@localhost bin]# ./splunk list forward-server
Active forwards:
        64.131.110.128:9997
```

Figure 3.11: Testeando la conexión en el forwarder.

3.3 Aprendiendo Queries Básicos

La barra de búsqueda de Splunk permite hacer búsquedas sobre información indexada.

Por ejemplo, el query **index=indexName** muestra toda la información relacionada a un índice específico. Si el usuario no crea ningún índice, toda la información es indexada al índice principal y este comando no es necesario.

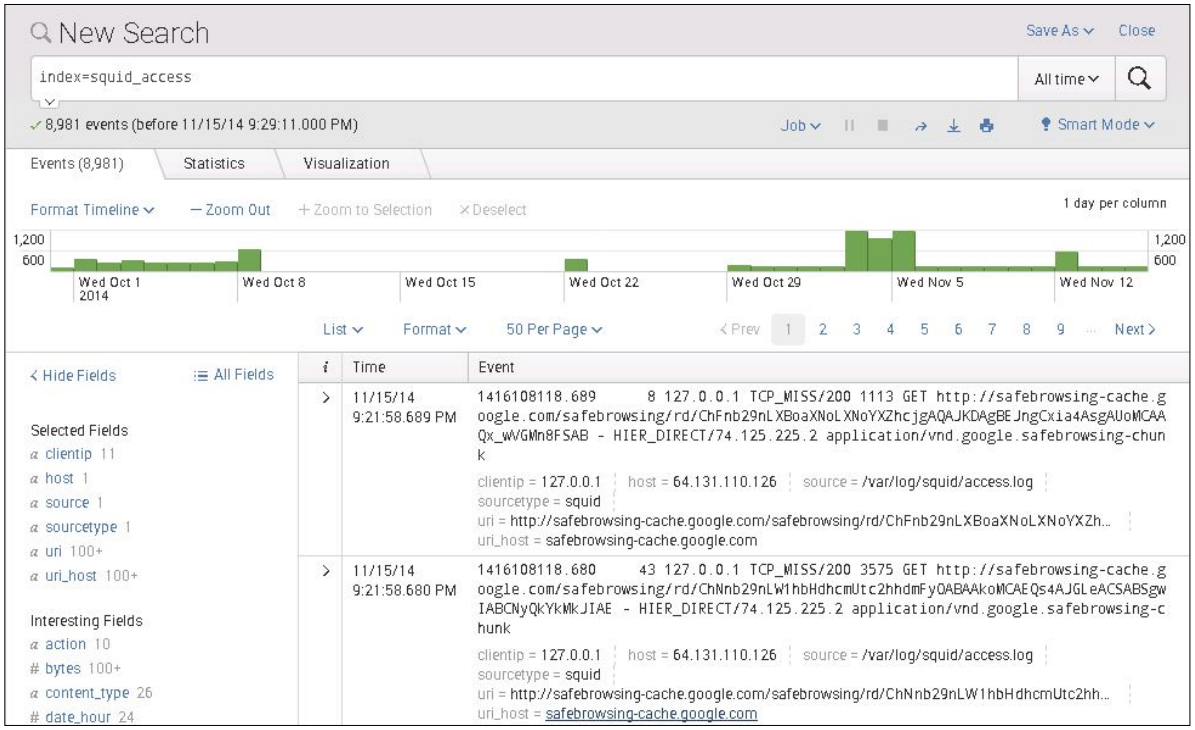


Figura 3.12: Resultados para "index=squid_access"

Query **index=indexName | search specific conditions**. Ya que un índice fue creado, toda búsqueda deberá empezar con index=indexName para obtener toda la información en ese índice. La búsqueda debería seguir con **| search** para aplicar condiciones específicas sobre los resultados del query index=indexName. Por ejemplo, un administrador desea ver todos los sitios web que el host 64.131.110.128 ha visitado. El host 64.131.110.128 es la condición que la información debe cumplir para ser presentada. Query **index=squid_access | search**

clientip="64.131.110.128" devuelve toda la información generada por el cliente con esa IP.

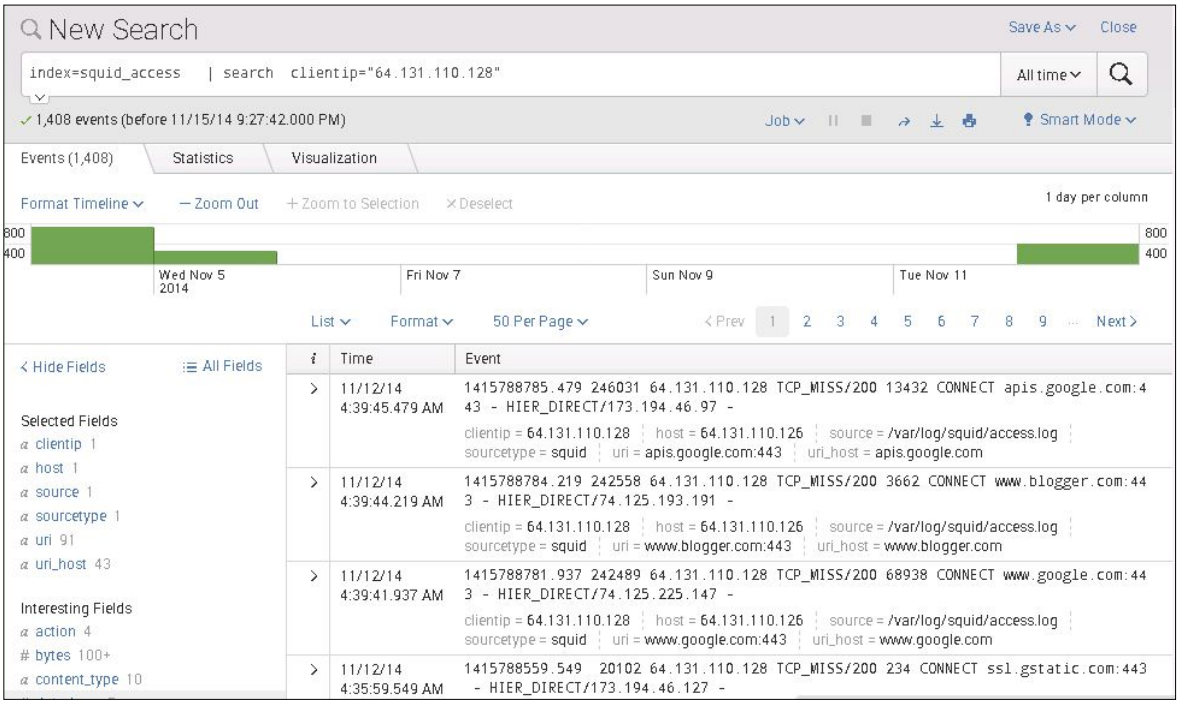


Figura 3.13: Resultados para el query index=squid_access | search clientip="64.131.110.128".

Query **index=squid_access | search uri="http://creditihabbogratuiti.blogspot.com/"** devuelve todas las visitas realizadas al sitio web, donde uri es el nombre del campo en squid para las URLs solicitadas por los usuarios.

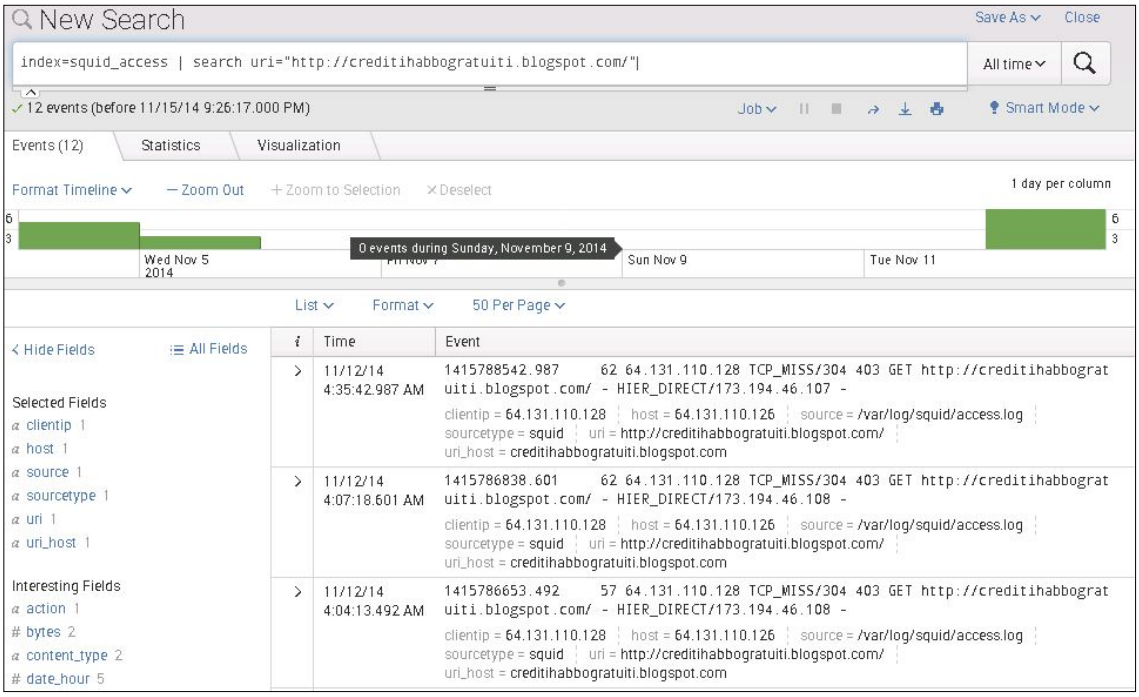


Figura 3.14: Resultados para el query index=squid_access | search uri="http://creditihabbogratuiti.blogspot.com/".

Squid para Splunk provee campos que facilitan las búsquedas sobre los archivos access.log. La siguiente figura en la parte izquierda muestra ejemplos de los campos reconocidos gracias a la aplicación Squid para Splunk.

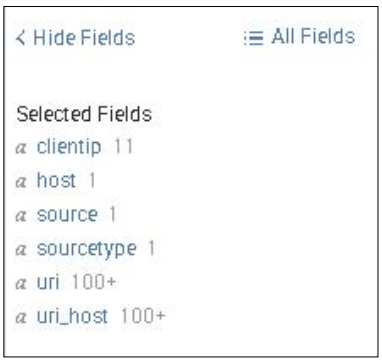


Figura 3.15: Ejemplo de campos reconocidos por squid app.

3.4 Alertas a sitios maliciosos

EL objetivo del proyecto es enviar alertas cuando un usuario visite sitios maliciosos en el preciso instante en que realiza el acceso. Esto ayudará a prevenir daños futuros a la red y a la organización en general.

Toda la información recibida del archivo access.log file es comparada en tiempo real con la lista de sitios maliciosos de Phishtank; si un usuario visita cualquier sitio de esta lista, la alerta se activará y el administrador recibirá un email con la dirección IP del usuario, la URL del sitio malicioso y el tiempo en que la alerta fue activada.

En el servidor Splunk (indexer), la aplicación GetWatchlist fue instalada para poder obtener la lista de Phistank desde el sitio web todos los días a la media noche y realizar comparaciones en tiempo real contra la información indexada. Dos tareas fueron creadas para cumplir con este objetivo: Updatecvs, la cual actualiza la PhishTank watchlist cada noche y la alerta malicious, la cual envía mails al administrador cada vez en un sitio de la lista es visitado.

3.4.1 Cargar Watchlist

Para cargar la listas de sitios maliciosos desde un sitio web en el servidor Splunk se debe realizar las siguientes configuraciones:

1. Abrir la interfaz web de Splunk e instalar Getwatchlist App desde https://apps.splunk.com/app/635/ de la misma forma en que la aplicación Squid fue instalada.

2. Cargar en Splunk la Phistank Watchlist.

   Click en **Apps -> Getwatchlist** y ejecutar la siguiente búsqueda:

```
| getwatchlist http://data.phishtank.com/data/online-valid.csv delimiter="," relevantFieldName=url relevantFieldCol=2 referenceCol=3 dateCol=4 categoryCol=8 ignoreFirstLine=true
```

Esta búsqueda obtiene la lista de sitios maliciosos de Phishtank donde **| getwatchlist http://data.phishtank.com/data/online-valid.csv** descarga el archivo desde el sitio web, **delimiter=","** específica que los datos son delimitados por comas, **relevantFieldName=url** específica que el campo más importante del archivo es la URL,

relevantFieldCol=2 específica que el campo URL está ubicado en la columna 2, **referenceCol=3 dateCol=4 categoryCol=8** describe los otros campos del archivo y **ignoreFirstLine=true** específica que no se debe incluir el nombre de las columnas.

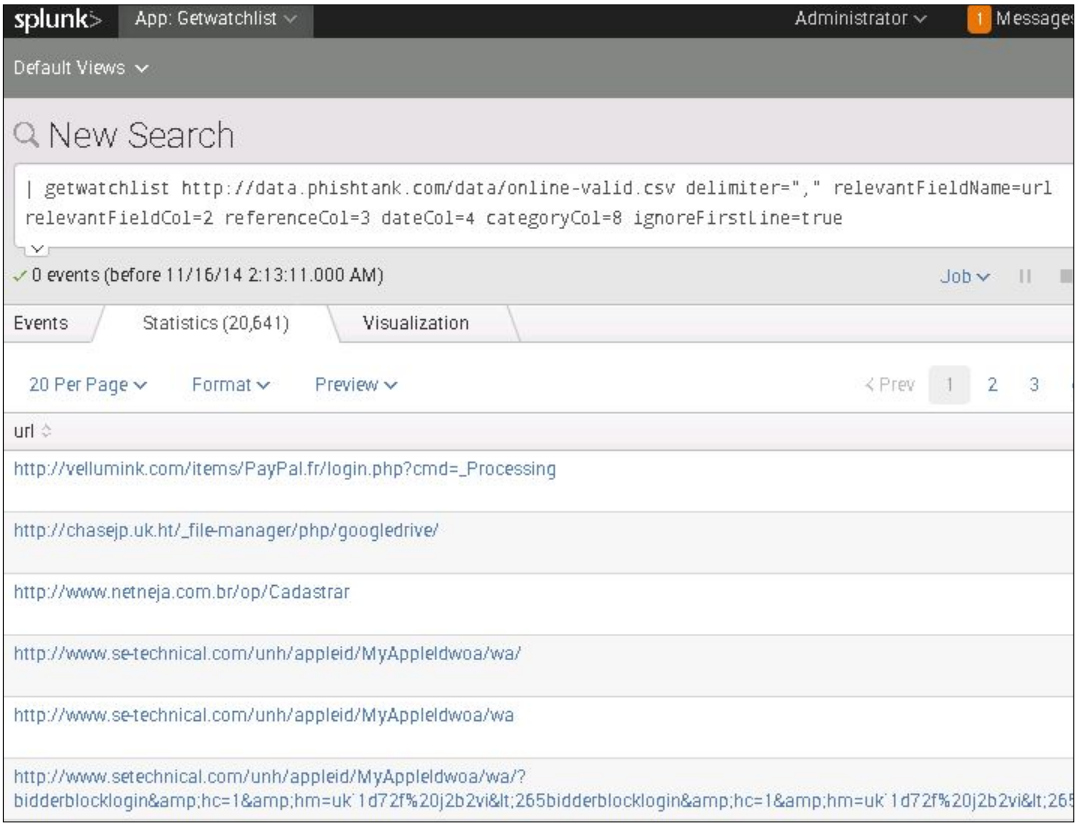


Figura 3.16: Watchlist obtenida en la Interfaz Web de Splunk.

3. Guardar la lista de sitios maliciosos de PhishTank en un archivo .csv.

El comando ejecutado en el literal anterior solamente muestra el listado en Splunk, para guardar la lista en un archivo csv es necesario añadir **| outputlookup phishtank.csv** al comando anterior como sigue:

```
| getwatchlist http://data.phishtank.com/data/online-valid.csv delimiter="," relevantFieldName=url relevantFieldCol=2 referenceCol=3 dateCol=4 categoryCol=8 ignoreFirstLine=true | outputlookup phishtank.csv
```

Donde phistank.csv es el archivo donde se almacenará la lista de sitios maliciosos (watchlist).

4. Actualizar el archivo Phishtank cada noche.

Es necesario crear una búsqueda programada a ejecutarse todos los días a la media noche para mantener el archivo actualizado, para lo cual se deben seguir los siguientes pasos..

4.1. Click en menú **Setting –> Search, reports and alerts**.

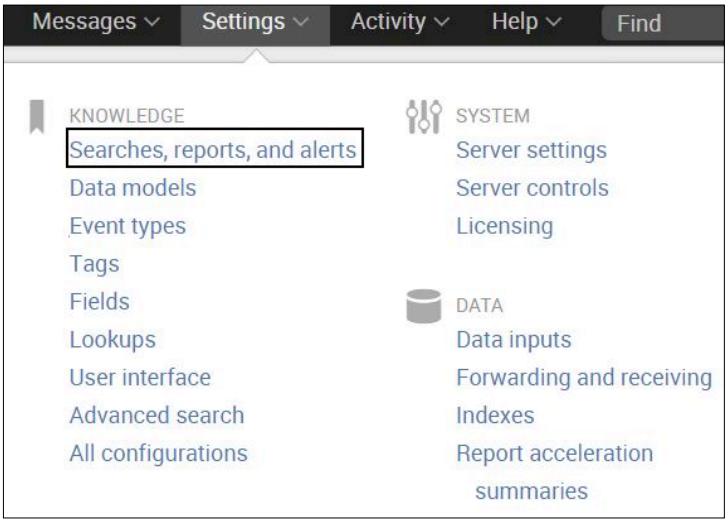


Figura 3.18: Paso 4.1

4.2. Click en **New** y crear nueva búsqueda programada.

En **Destination App**, seleccione **Getwatchlist.**

Escriba el nombre de la alerta en **Search Name: updatecsv**

En **Search** coloque el comando anterior.

Seleccione la opción **Schedule this search**.

En **Run every**, escoja **day at midnight,** deje el resto de valores por default y seleccione guardar **(save).**

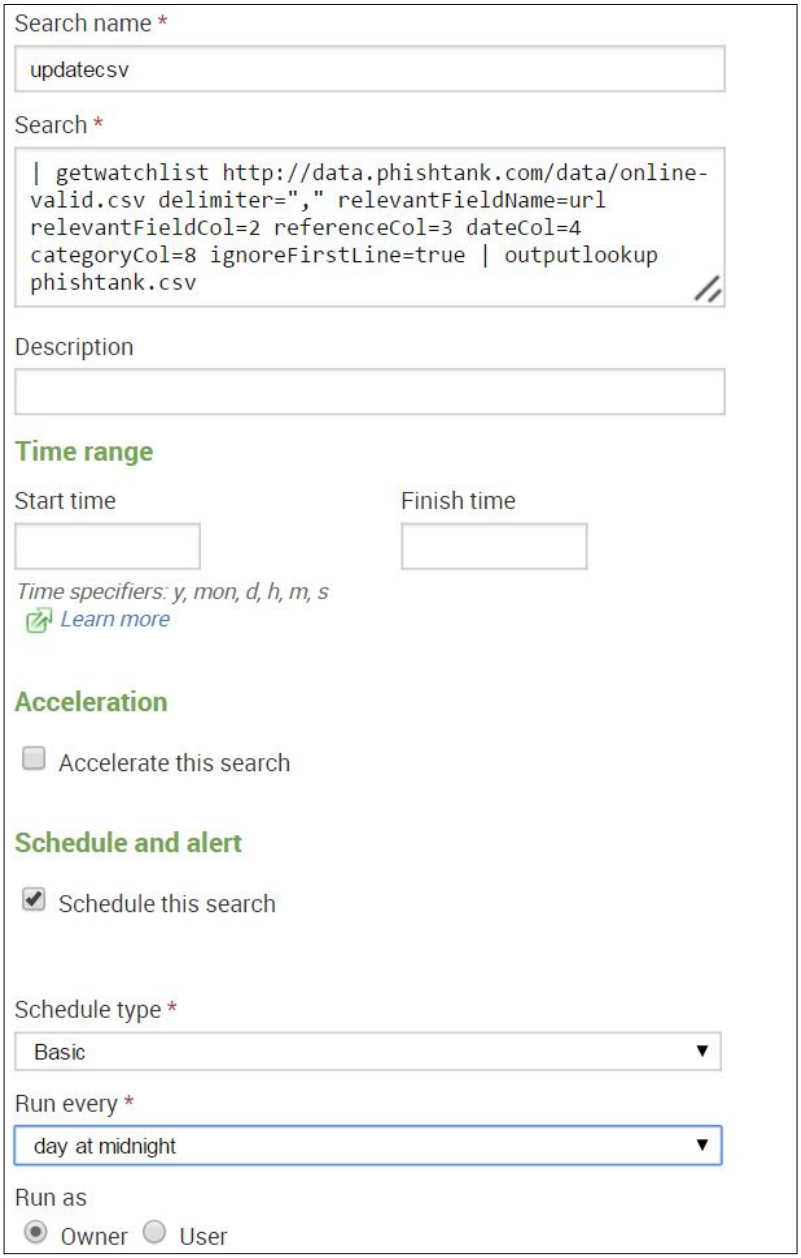


Figura 3.19: Paso 4.2.

3.4.2 Crear alertas

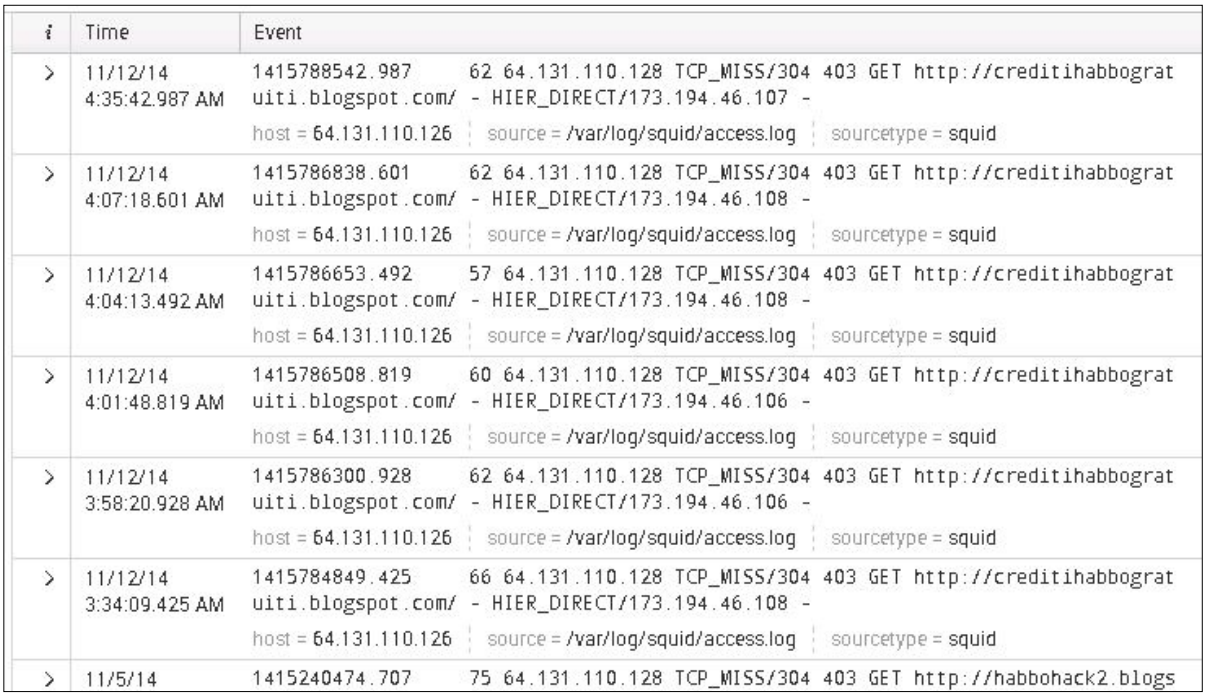
En la interfaz Web de Splunk:

1. Buscar por cualquier acceso a sitios maliciosos de la lista PhishTank.

En **Apps -> Getwatchlist** ejecute la siguiente búsqueda:

```
index=squid_access [ | inputlookup phishtank.csv | rename url as uri | fields uri]
```

Esta búsqueda devuelve todos los usuarios que han visitado sitios que se encuentran en la lista de sitios maliciosos (phistank.csv), donde **index=squid_access** devuelve todos los datos en el índice squid y **[| inputlookup phishtank.csv | rename url as uri | fields uri]** compara la URL accedida a través de squid con el archivo csv. **Inputlookup phishtank.csv** específica el nombre de el archivo usado para la comparación. **Rename url as uri** renombra el campo URL como URI porque en squid el campo URL es llamado URI. **Fields uri** especifica que la comparación se haga usando el campo URI.



i	Time	Event
>	11/12/14 4:35:42.987 AM	1415788542.987 62 64.131.110.128 TCP_MISS/304 403 GET http://creditihabbograt uiti.blogspot.com/ - HIER_DIRECT/173.194.46.107 - host = 64.131.110.126 source = /var/log/squid/access.log sourcetype = squid
>	11/12/14 4:07:18.601 AM	1415786838.601 62 64.131.110.128 TCP_MISS/304 403 GET http://creditihabbograt uiti.blogspot.com/ - HIER_DIRECT/173.194.46.108 - host = 64.131.110.126 source = /var/log/squid/access.log sourcetype = squid
>	11/12/14 4:04:13.492 AM	1415786653.492 57 64.131.110.128 TCP_MISS/304 403 GET http://creditihabbograt uiti.blogspot.com/ - HIER_DIRECT/173.194.46.108 - host = 64.131.110.126 source = /var/log/squid/access.log sourcetype = squid
>	11/12/14 4:01:48.819 AM	1415786508.819 60 64.131.110.128 TCP_MISS/304 403 GET http://creditihabbograt uiti.blogspot.com/ - HIER_DIRECT/173.194.46.106 - host = 64.131.110.126 source = /var/log/squid/access.log sourcetype = squid
>	11/12/14 3:58:20.928 AM	1415786300.928 62 64.131.110.128 TCP_MISS/304 403 GET http://creditihabbograt uiti.blogspot.com/ - HIER_DIRECT/173.194.46.106 - host = 64.131.110.126 source = /var/log/squid/access.log sourcetype = squid
>	11/12/14 3:34:09.425 AM	1415784849.425 66 64.131.110.128 TCP_MISS/304 403 GET http://creditihabbograt uiti.blogspot.com/ - HIER_DIRECT/173.194.46.108 - host = 64.131.110.126 source = /var/log/squid/access.log sourcetype = squid
>	11/5/14	1415240474.707 75 64.131.110.128 TCP_MISS/304 403 GET http://habbohack2.blogs

Figura 3.20: Resultados para la búsqueda index=squid_access [| inputlookup phishtank.csv | rename url as uri | fields uri]

2. Guardar la búsqueda como una alerta en tiempo real.

2.1. Click en **Save As -> Alert**

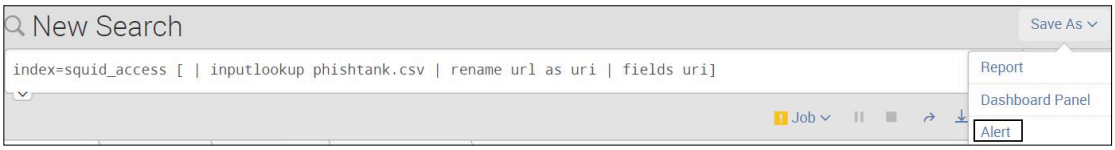


Figura 3.21: Step 2.1

2.2. Ingrese el nombre de la alerta: **malicious**, click en **Real Time** y Next

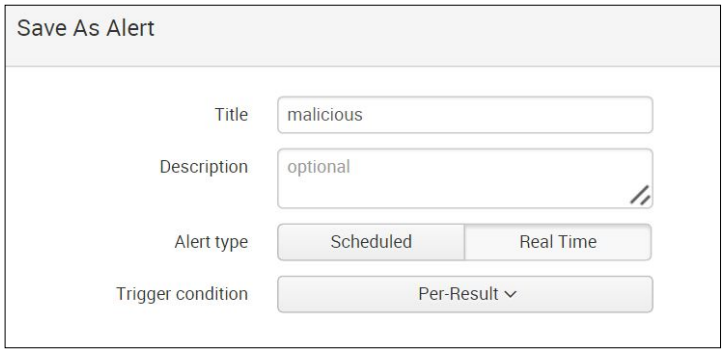


Figura 3.22: Paso 2.2

2.3. Seleccione **List on Triggered Alerts**

2.4. Seleccione **Send Email** e ingrese el correo del administrador **To: icarrer2@hawk.iit.edu**

2.5. Seleccione todas las opciones mostradas en **Include** y **Save**

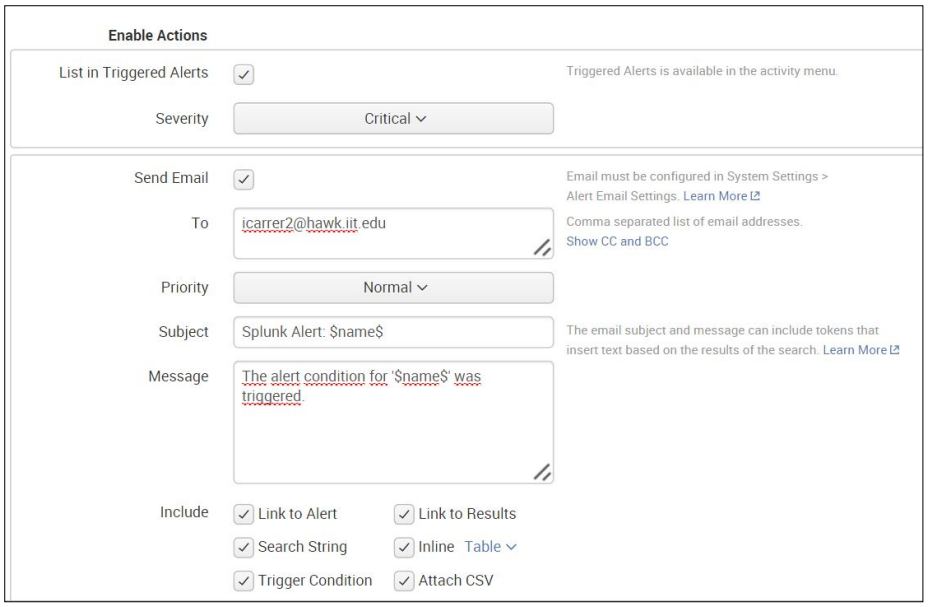


Figura 3.23: Paso 2.3 a 2.5

3. Configurar el servidor SMTP con el fin de permitir que el servidor Splunk envíe correos al administrador cuando una alerta se active.

    3.1. Click en **Settings > System Settings > Email Settings**

    3.2. Configurar mail host como **smtp.gmail.com**. En este caso, los correos del IIT utilizan el forwarder de Gmail.

    3.3. Una dirección de correo y contraseña debe ser configurada. En este caso, se usa el correo de Ivette Carrera.

    3.4. Escribir **adminSplunk** para Link hostname.

    3.5. Escribir **Splunk** en “Send emails as” para saber que los emails provienen de Splunk.

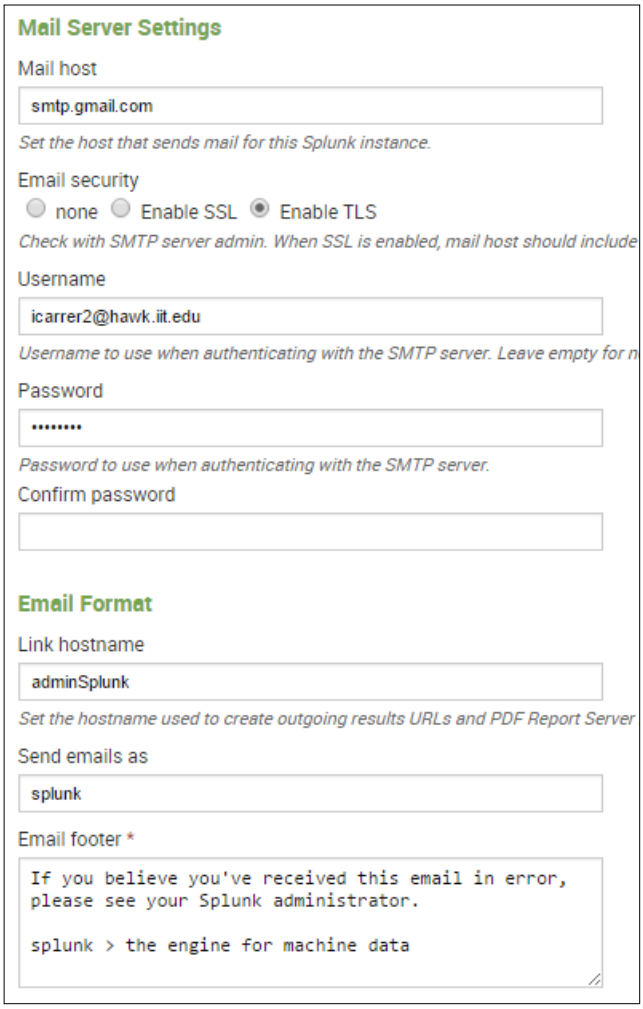


Figure 3.24: Paso 3.1 a 3.5

CAPÍTULO 4

PRUEBAS

4.1 Escenario

Juan, un usuario de la organización XYZ, recibe un mail de notificación de Facebook en su cuenta de correo personal. El correo aparenta proceder de Facebook diciendo que alguien ha comentado una de las fotos de Juan; “Diana made a comment about your photo” era el asunto del correo. El asunto del correo es una notificación común que envía facebook cuando alguien realiza un comentario en una foto.

Un usuario común no pensaría que hay algo extraño en este correo y

lo abriría sin pensarlo dos veces. El correo contiene un link para que "el usuario pueda ver el comentario" sobre su foto. Juan dio click sobre el link sin dudarlo y fue redireccionado a otro sitio web pero esta redirección no causa ninguna preocupación en Juan. Juan ignora lo ocurrido y continua trabajando sin conocer que realmente sucedió.

Juan no se percató que la notificación es un correo falso y que el link lo redireccionó a un sitio malicioso que instaló un malware en su computadora y le robó su información personal.

Figura 4.1: Notificación falsa de Facebook recibida en el correo de Juan.

Figura 4.2: Sitio malicioso al que se redireccionó a Juan.

La organización XYZ ha implementado la solución propuesta en este proyecto y tiene creadas alertas en contra de esta acción trabajando en tiempo real. Cuando Juan dio click en el link, una alerta fue enviada se active y el administrador de la red recibió un correo con la notificación de una posible infección. Esta notificación contiene la dirección IP del usuario que disparó la alerta, el sitio web visitado y el tiempo en que ocurrió el evento.

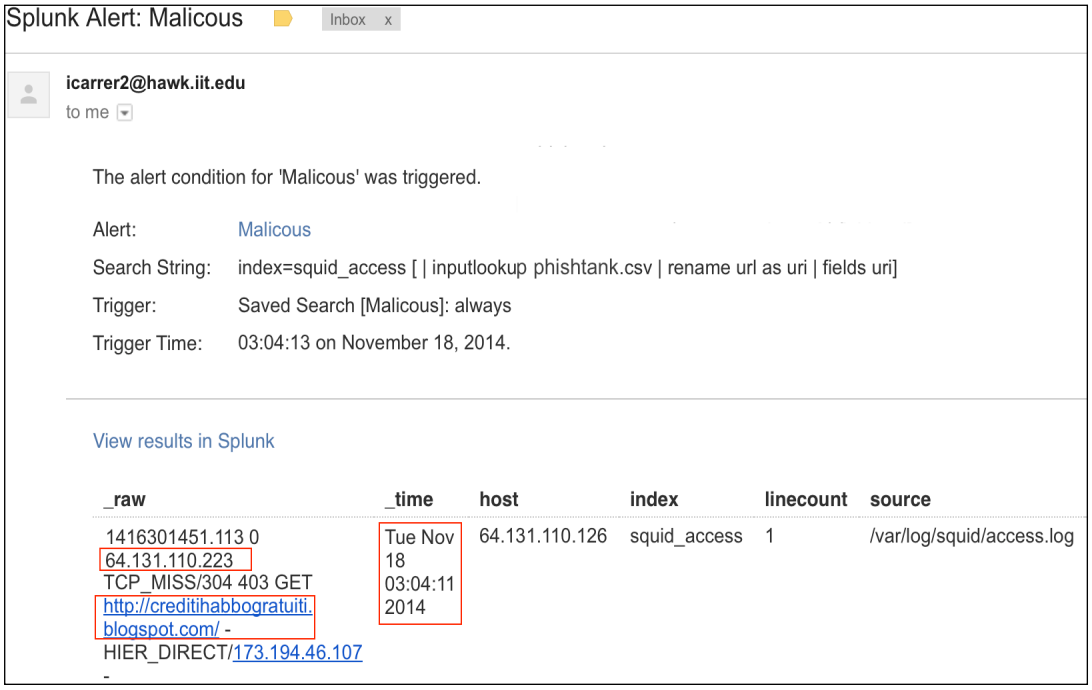


Figura 4.3: Email enviado al administrador.

La Figura 4.4 muestra que el sitio web al que fue redireccionado Juan se encuentra en la lista de sitios web maliciosos, de manea que la alarma se accionó propiamente.

El administrador debería aislar la máquina de la red como primera respuesta para evitar que otros equipos se infecten y luego empezar a indagar sobre lo ocurrido.

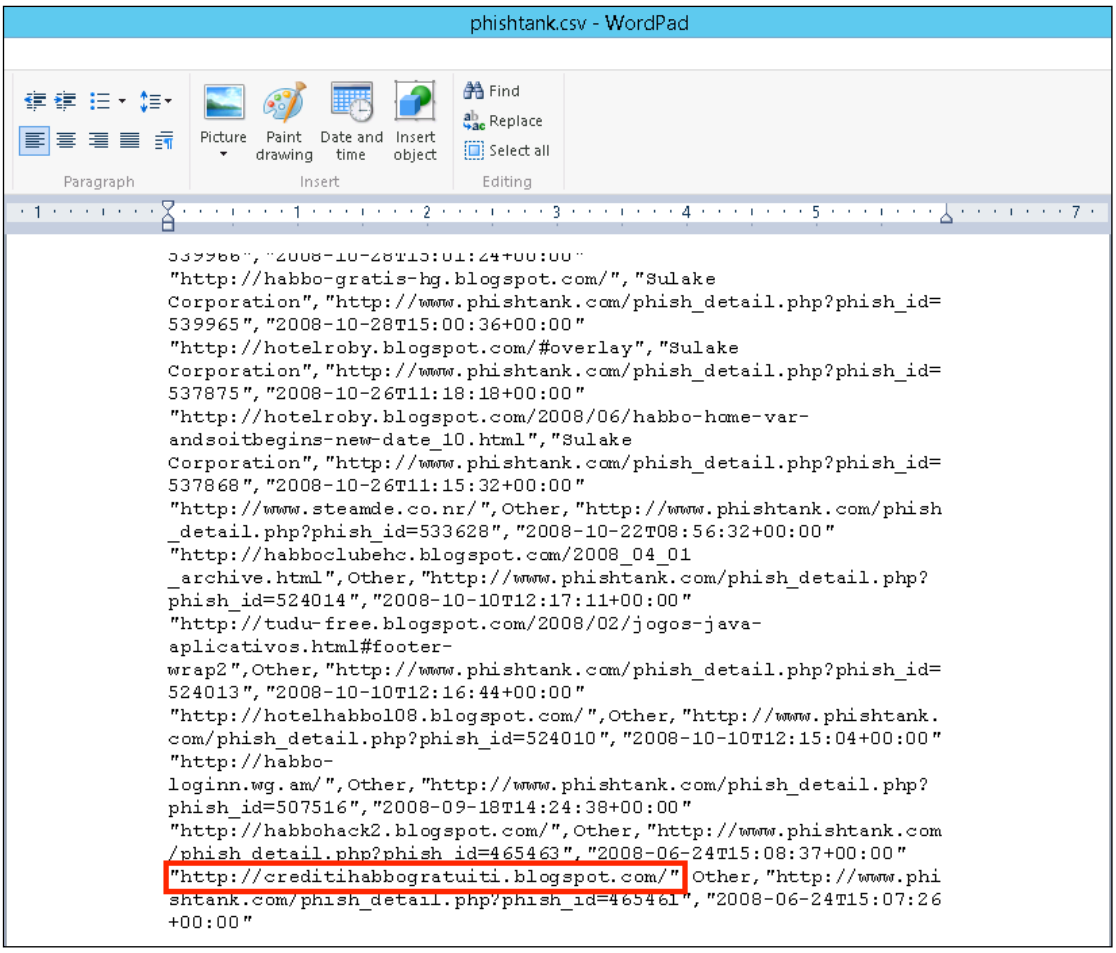


Figura 4.4: Archivo Phistank.csv (watchlist).

En este proyecto solamente se esta indexando datos desde el servidor proxy, limitándolo a búsquedas relacionadas a esta información, como por ejemplo: Qué otro equipo podría estar infectado? o Qué otros sitios ha visitado la victima? Pero, si adicionalmente se hubieran indexado los logs provenientes de sistemas de seguridad como un IDS o Antivirus, un administrador podría fácilmente identificar el propósito del correo y que realmente hizo en el equipo. Este alcance provee una completa figura de

la infraestructura, considerando que cualquier búsqueda realizada será sobre toda la información relativa a logs de seguridad; lo que permitirá que las amenazas sean fácilmente combatidas.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. Debido al creciente aumento de crímenes informáticos es necesario contar con medidas de seguridad que permitan contener posibles ataques.

2. Aplicaciones, servidores, dispositivos de seguridad en las redes, etc. generan diariamente millones de entradas en los logs. Esta información generada es valiosa en el momento de realizar un análisis de seguridad.

3. En el momento en que ocurre un evento de seguridad, el administrador o analista tendrá que analizar cada dispositivo de la red para poder

determinar lo que está pasando, razón por la cual además de dispositivos de seguridad es necesario tener una plataforma donde se indexen todos los logs generados por estos dispositivos de manera que la búsqueda sobre ellos sea mucho más rápida.

4. Splunk provee herramientas útiles de análisis de información que permiten detectar posibles infecciones en la red como es el caso de las alertas. La creación de alertas cuando usuarios acceden a sitios maliciosos permiten al administrador evitar que toda su red se afecte por algún malware ya que le permitirá responder casi instantáneamente.

5. Splunk junto con los logs de los distintos dispositivos de seguridad forman una herramienta poderosa haciendo muy difícil que un atacante se infiltre en la red o la perjudique.

6. El caso de estudio simulado demuestra la utilidad del proyecto evitando la propagación del malware en toda la red.

Recomendaciones:

1. Implementar un sistema de autenticación de usuarios para poder realizar la búsqueda por usuarios y no por IPs.

2. En el proyecto solo se incluyeron los logs provenientes de Squid, pero se recomienda incluir todos los logs generados por los dispositivos de seguridad para implementar una solución más robusta.

3. Realizar una campaña de concientización al personal de la organización sobre sitios maliciosos y las repercusiones de visitar estos sitios con el fin de evitar el acceso intencional a los mismos. Así como también, sobre los posibles ataques a los que están expuestos para que no sean blancos fáciles para los atacantes.

BIBLIOGRAFÍA

[1] Kent Karen & Murugiah Souppaya (2006), *Guide to Computer Security Log Management* (Special Publication), National Institute of Standards and Technology.Retrieve

From :http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[2] Splunk Inc(2012), *About Splunk Enterprise deployments*. From: http://docs.splunk.com/Documentation/Splunk/latest/Overview/AboutSplunkEnterprisedeployments

[3] Splunk Inc (2012), *About the search Dashboard*. From :http://docs.splunk.com/Documentation/Splunk/6.2.0/SearchTutorial/Aboutthesearchapp

[4] Splunk Inc.. *Getwatclist Overview*.

From: https://apps.splunk.com/app/635/

[5] Squid Org., *Squid: Optimizing Web Delivery*,

From: http://www.squid-cache.org/

[6] Apache Org., *Working with Log Files*, From: https://docs.trafficserver.apache.org/en/latest/admin/working-log-files.en.html

[7] PhishTank Org., *What is PhishTank?*

From :https://www.phishtank.com/index.php

[8] Splunk Inc., *Splunk Doc--Configure CSV and external lookups*, From :

http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Addfields

fromexternaldatasources