Dom. Cien., ISSN: 2477-8818
Vol. 3, núm. 4, julio, 2017, pp. 721-751

Número Publicado el 15 de julio de 2017

DOI: 10.23857/dc.v4i3 Especial.585

Ciencias Eléctricas

Artículo Científico

Implementación de una plataforma de detección de accesos a sitios maliciosos

Implementation of a platform to detect access to malicious sites

A implementação de um acesso plataforma de detecção para sites maliciosos

Ivette K. Carrera-Manosalvas [I]
Ivette.carreram@ug.edu.ec

Eduardo S. Cruz-Ramírez [II]
escruz@espol.edu.ec

Ginger V. Saltos-Bernal [III]
gvsaltos@espol.edu.ec

Recibido: 30 de enero de 2017 ***** **Corregido:** 20 de febrero de 2017 ***** **Aceptado:** 20 junio de 2017

I. Ingeniera En Telemática; Master Of Cyber Forensics And Security; Magister En Seguridad Informática Aplicada; Universidad De Guayaquil, Guayaquil, Ecuador.

II. Ingeniero En Ciencias Computacionales; Magister En Seguridad Informática Aplicada; Escuela Superior Politécnica Del Litoral, Guayaquil, Ecuador.

III. Ingeniera En Telemática; Master Of Science In Forensic Information Technology; Magister En Seguridad Informática Aplicada; Escuela Superior Politécnica Del Litoral, Guayaquil, Ecuador.

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 cómo 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.

Palabras clave: plataforma; detección; sitios maliciosos; servidor

Abstract

The present work shows the implementation of an access detection platform for malicious sites in a previously configured test environment.

The first chapter details the problem to be solved as well as the proposed solution. Subsequently, the theoretical concepts necessary for the execution of the project are clarified.

The third chapter specifies step by step the installations and configurations that must be performed on both the proxy server and the Splunk server, as well as the proxy configuration on the machine that simulates the user. For the creation of alerts, first explains how to perform basic searches on the indexed information and then proceed to perform searches compared to a list of malicious sites previously downloaded.

Finally, tests are performed simulating a phishing attack to a user in order to verify the correct operation of the project.

Key words: platform; detection; Malicious sites; server

Resumo

Este trabalho apresenta a implementação de um acesso plataforma de detecção para sites maliciosos em um ambiente de teste previamente definido.

No primeiro capítulo e resolver o problema como a solução proposta detalhada. Em seguida, ele passa a esclarecer conceitos teóricos necessários para a implementação do projeto.

No específico da instalação terceiro capítulo passo-a-passo e configuração para executar o servidor proxy e o servidor Splunk, bem como configurações de proxy na máquina que simula o usuário. Para a criação de alertas, primeiro explica como realizar pesquisas básicas sobre a informação indexada e depois prosseguir para procurar comparando-os com uma lista de sites maliciosos previamente baixados.

Finalmente, os testes são realizados simulando um ataque de phishing um utilizador, a fim de verificar o funcionamento correcto do projecto.

Palavras chave: plataforma; detecção; sites maliciosos; servidor

Introducción.

El crecimiento de los ataques (Dussan Clavijo, 2006) informáticos (M, 2010) (Salvadori, 2013)así como su complejidad ha creado la necesidad de encontrar maneras que permitan responder de manera inmediata a posibles ataques (Melo, 2008). Toda la información generada por (Herrera Burgos, 2012) aplicaciones, (ESPINAL, MONTOYA, & ARENAS, 2010)servidores (Durán, Mondragón M., & Sánchez M., 2008), dispositivos de seguridad en las redes, (Baluja-García & Anías-Calderón, 2006) 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 (Jacovkis, 2011) 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

Materiales y métodos.

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 disparó alerta, es enviada al analista de seguridad.

Resultados.

IMPLEMENTACIÓN

Ambiente de Prueba

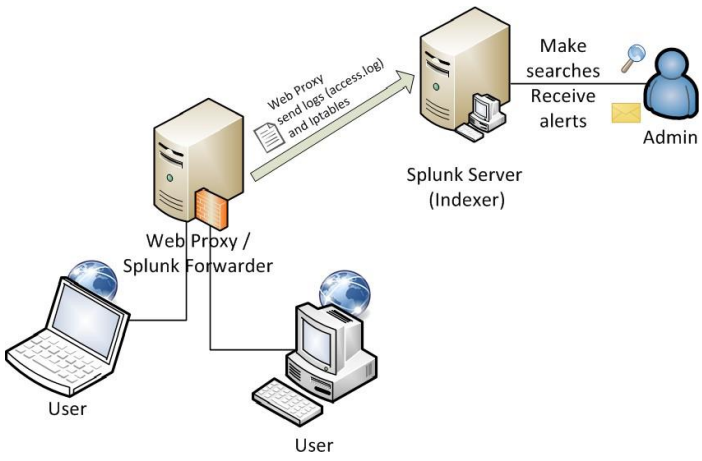


Figura 1: Ambiente del Proyecto

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.

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

Tabla 1: Características del Servidor Splunk

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.

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)

Tabla 2: Características del Servidor Web Proxy

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.

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 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.
```

Figura 3

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.

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.

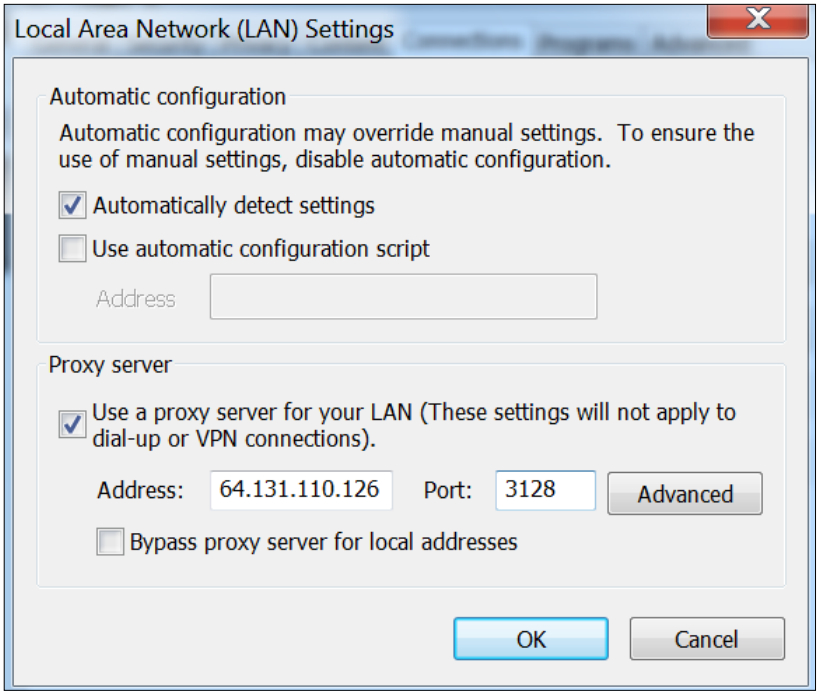


Figura 4: Internet Explorer – configuración Web Proxy.

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.

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.

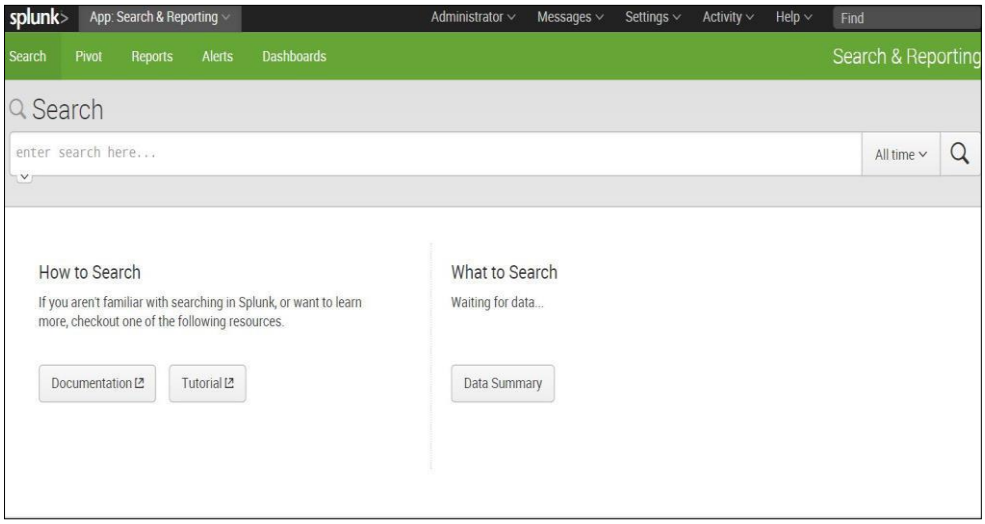


Figura 5: Interfaz Web principal de Splunk

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.

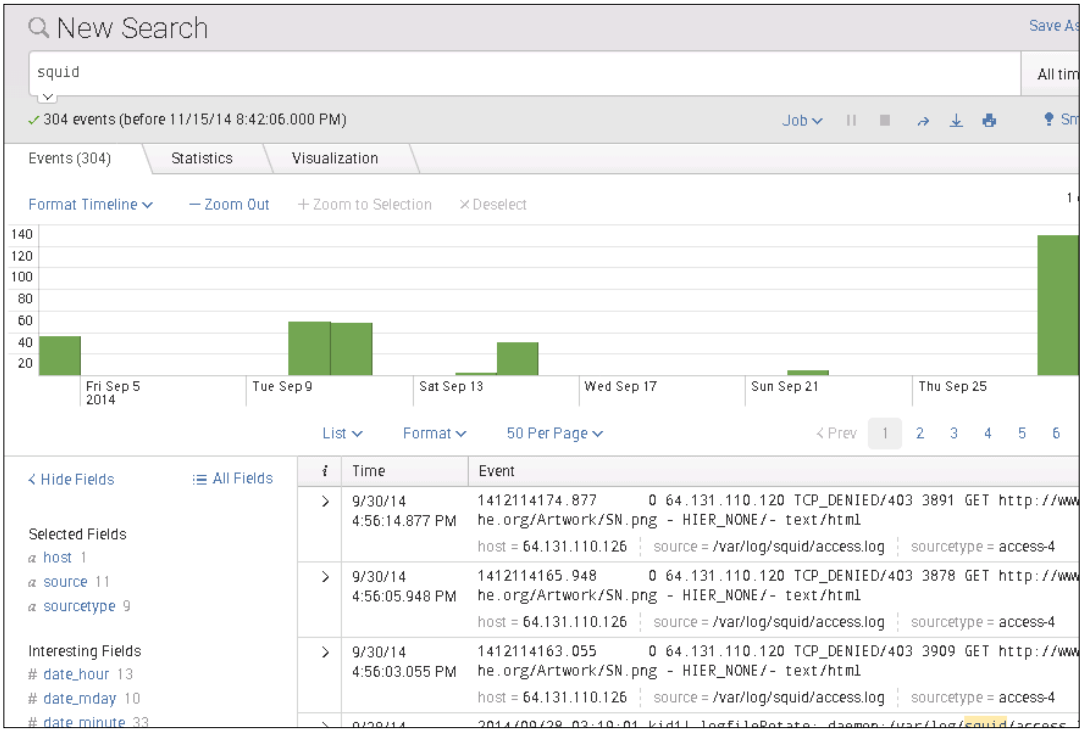


Figura 6: Datos recibidos desde el servidor Web Proxy.

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

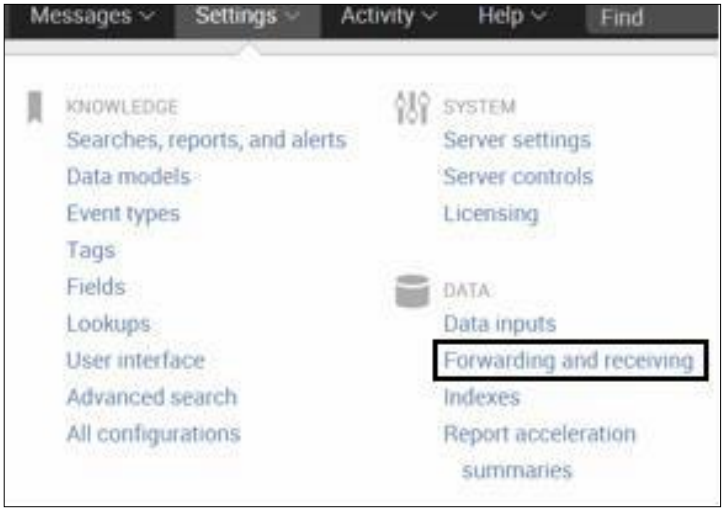


Figura 7: Paso 3.1

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

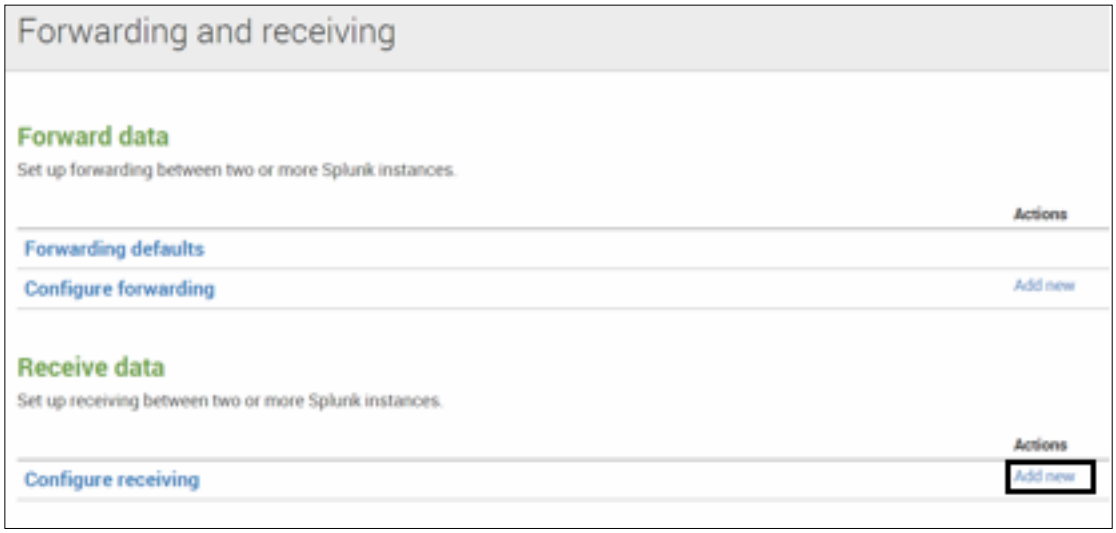


Figura 8: Paso 3.2

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

Figure 9: 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

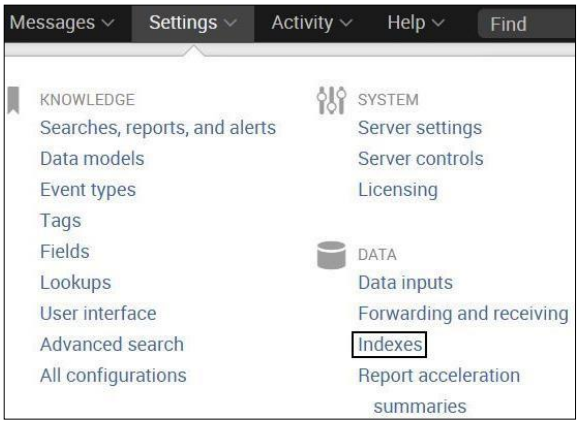


Figura 10: Paso 5.1

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.

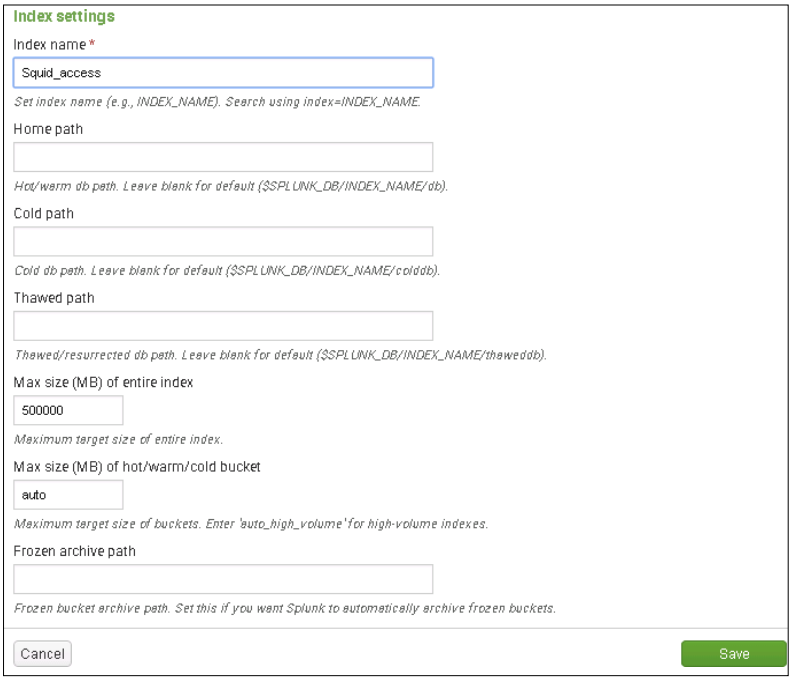


Figura 11: Paso 5.2

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
```

Imagen 12

8. Probar la conexión en el Forwarder

Ejecutar ./splunk list forward-server

La Figura 13 muestra que la conexión con el indexer está activa.

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

Figure 13: Testeando la conexión en el forwarder.

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.

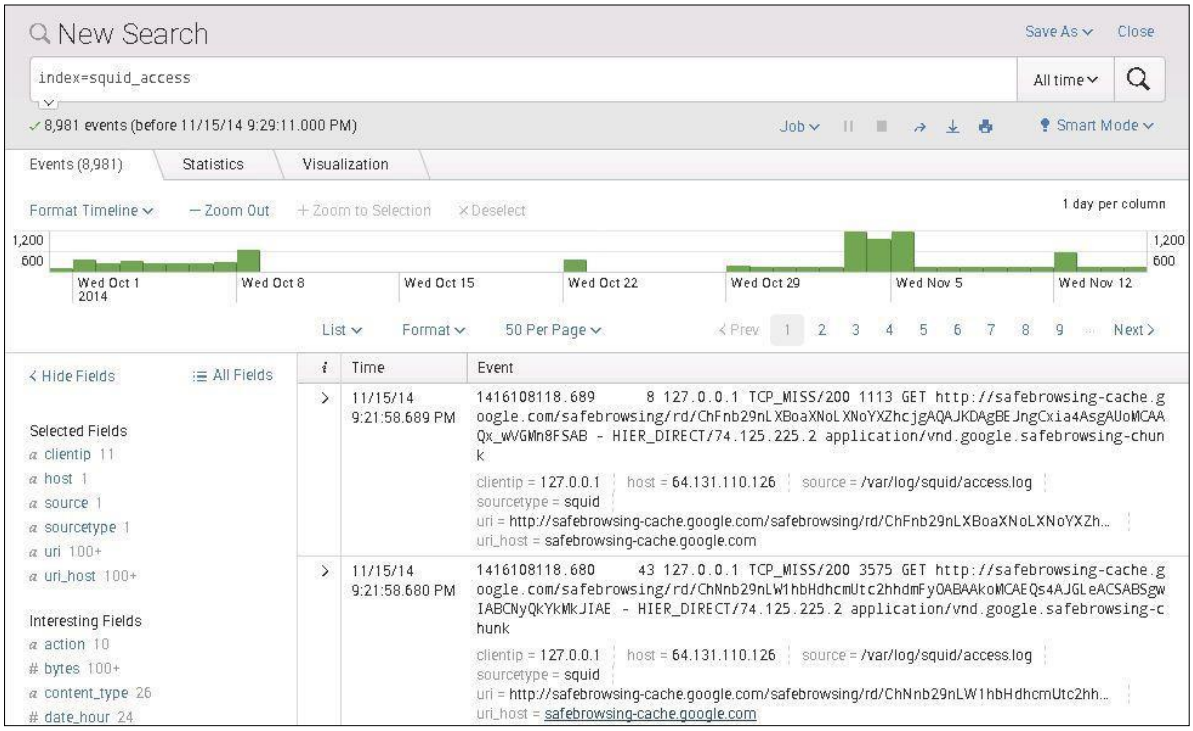


Figura 14: Resultados para "index=squid_access"

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.

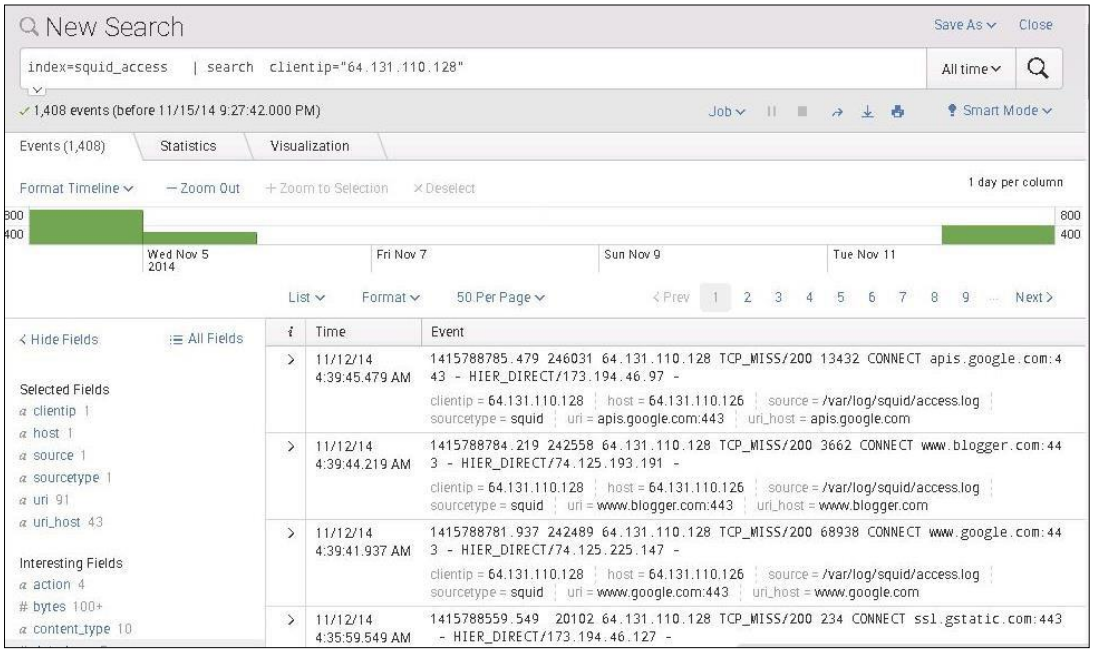


Figura 15: Resultados para el query index=squid_access | search clientip="64.131.110.128".

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.

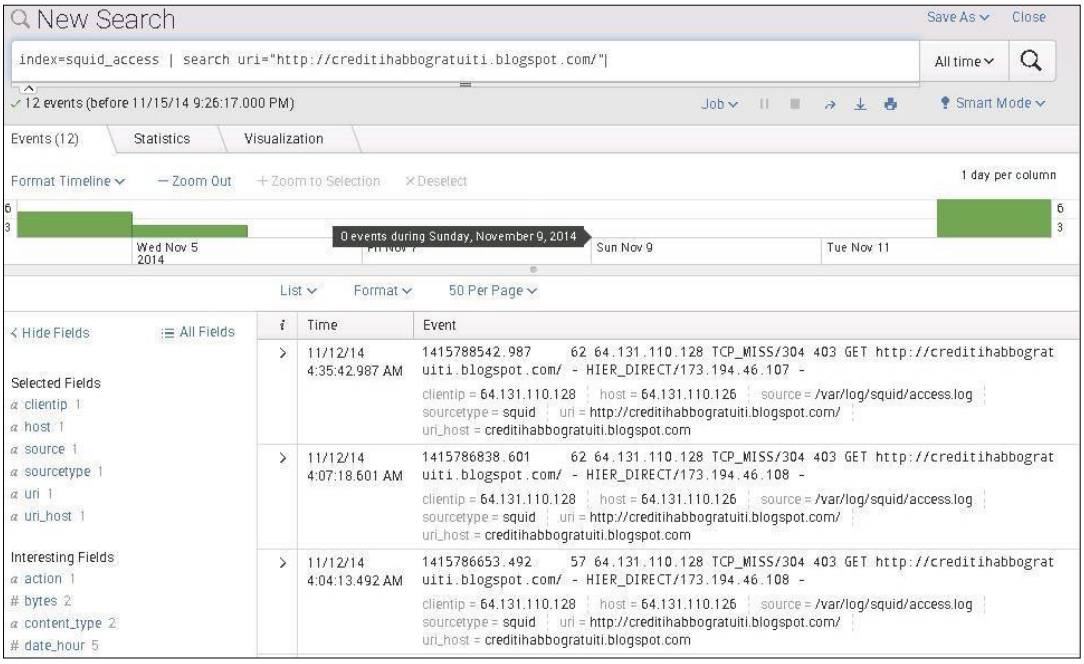


Figura 16: Resultados para el query index=squid_access | search uri="http://creditihabbogratuiti.blogspot.com/".

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.

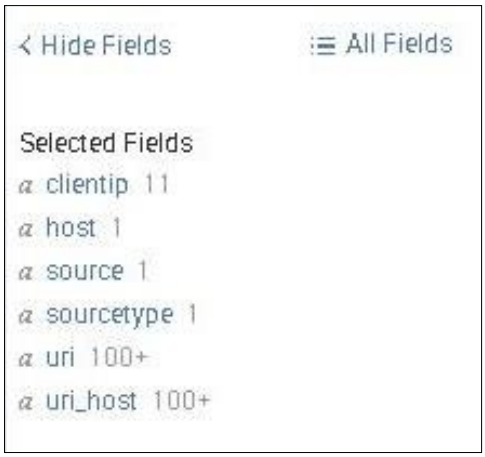


Figura 17: Ejemplo de campos reconocidos por squid app.

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.

Cargar Watchlist

Para cargar las 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
```

Figura 18

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.

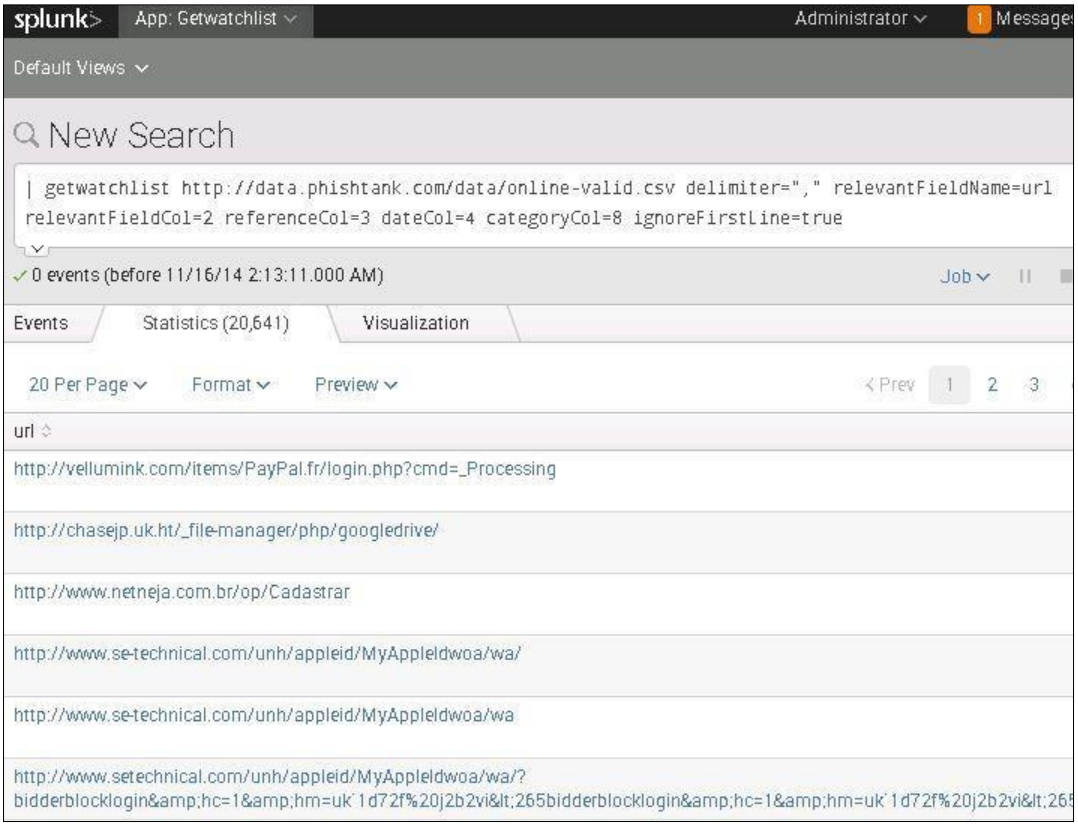


Figura 19: Watchlist obtenida en la Interfaz Web de Splunk.

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
```

Figura 20

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

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.

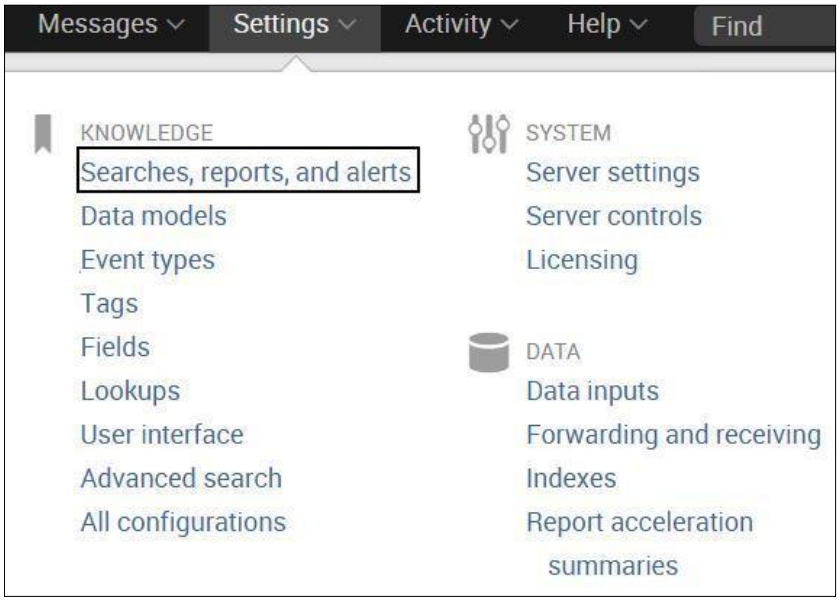


Figura 21: Paso 4.1

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).

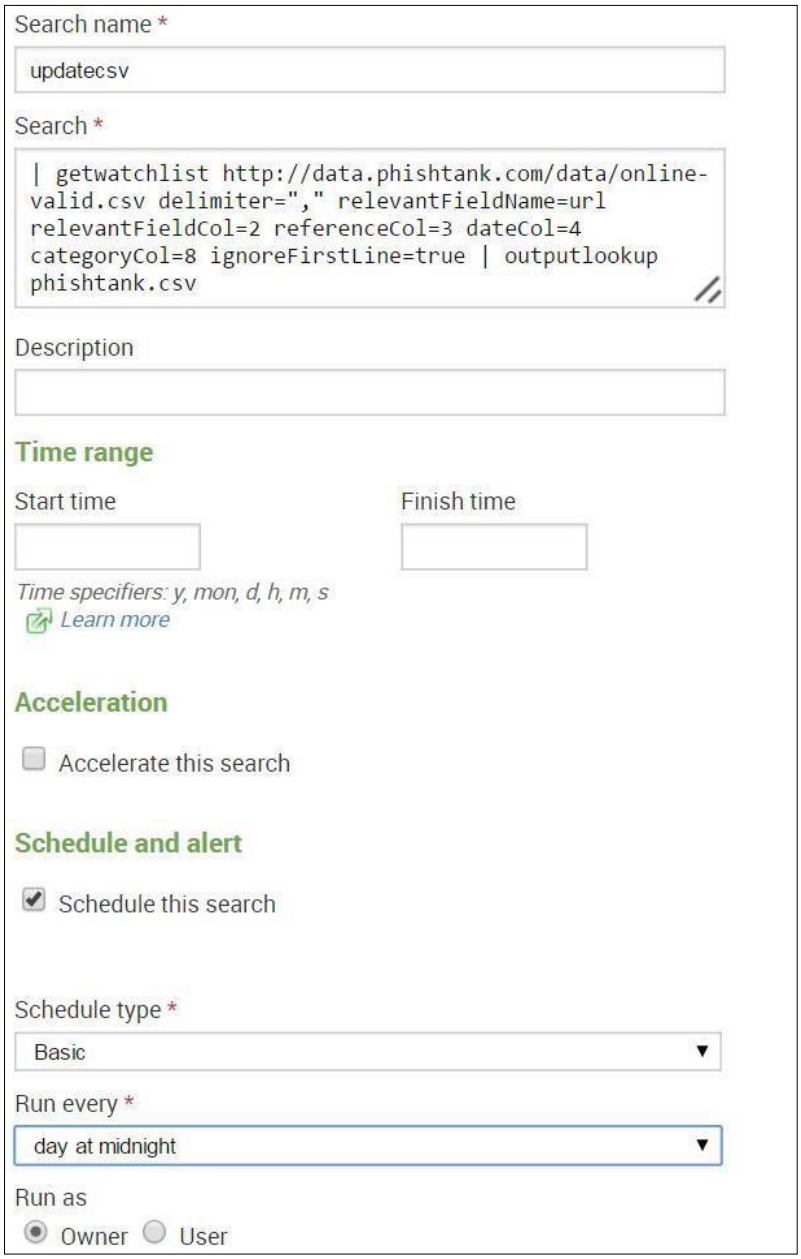


Figura 22: Paso 4.2.

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]
```

Figura 23

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 24: 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 25: Step 2.1

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

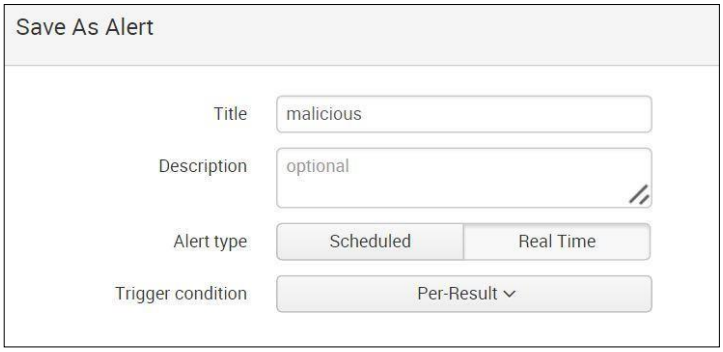


Figura 26: Paso 2.2

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

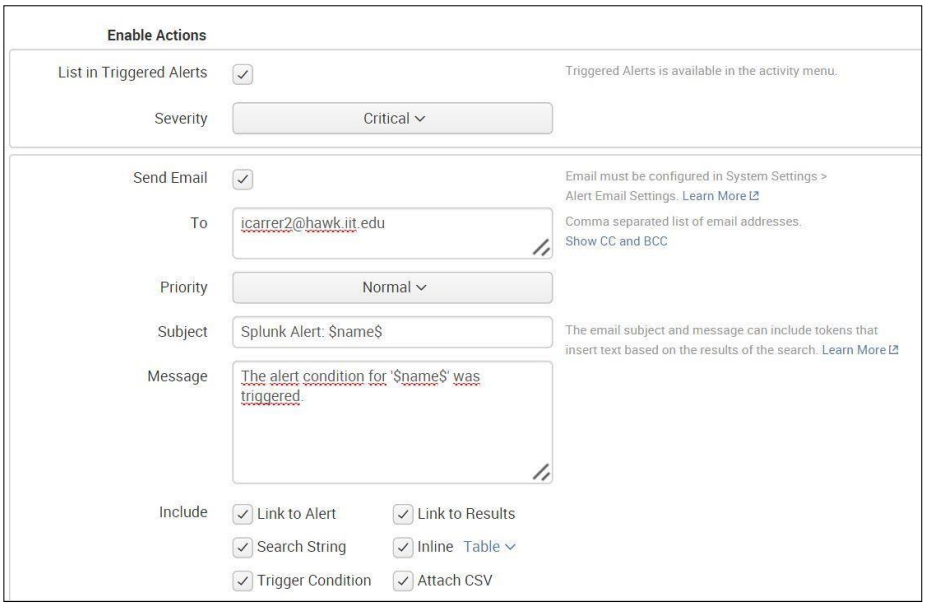


Figura 27: Paso 2.3 a 2.5

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.

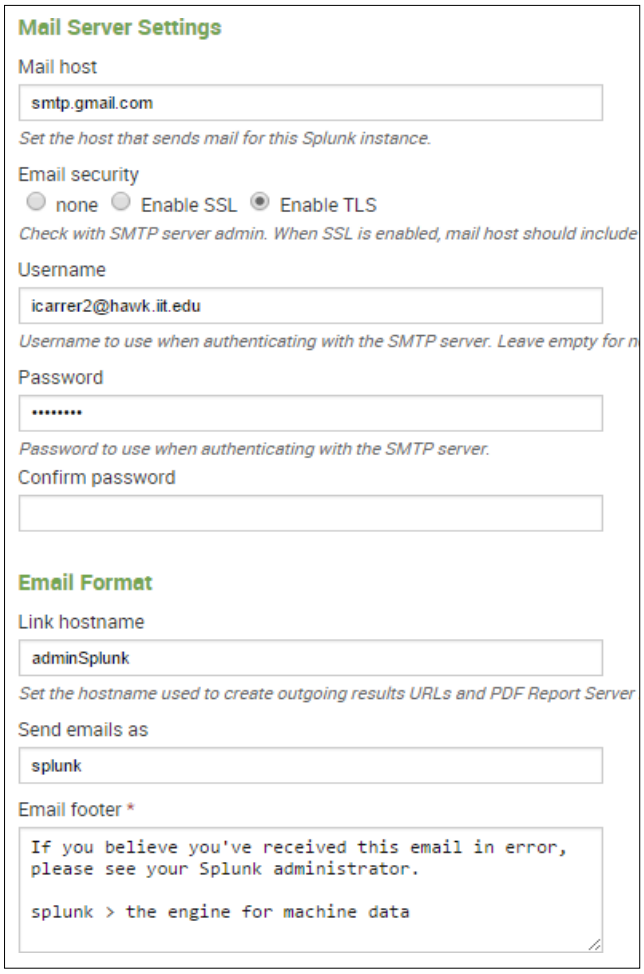


Figure 28: Paso 3.1 a 3.5

PRUEBAS

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

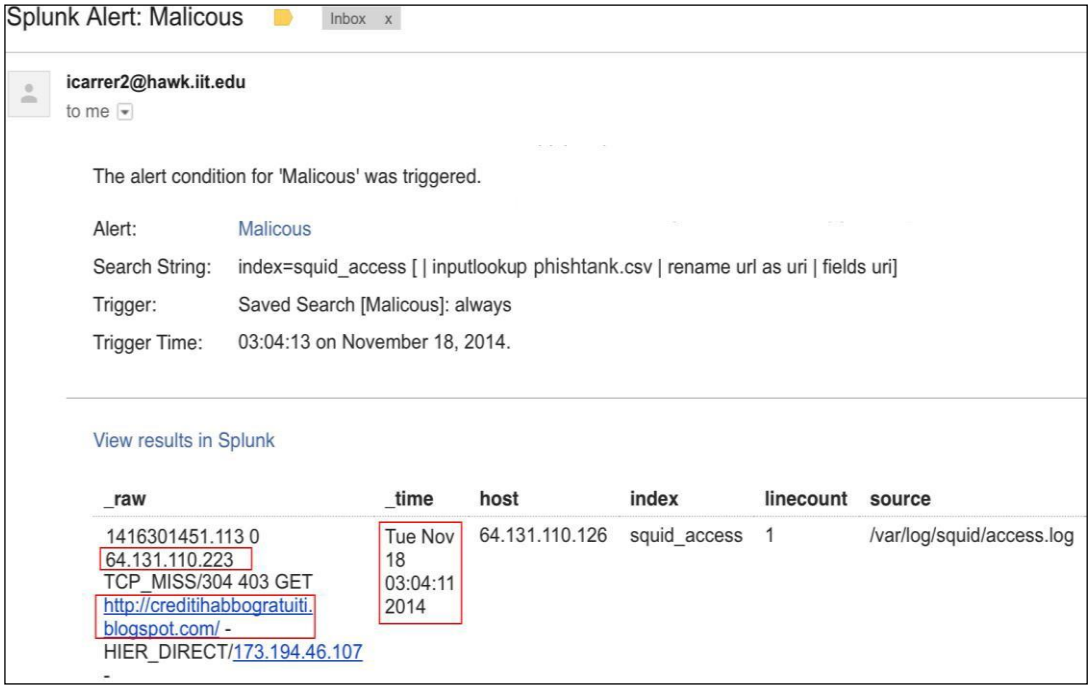
no causa ninguna preocupación en Juan. Juan ignora lo ocurrido y continua trabajando sin conocer que realmente sucedió.

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 29: Notificación falsa de Facebook recibida en el correo de Juan.

Figura 30: 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.


Splunk Alert: Malicous Inbox x

icarrer2@hawk.iit.edu
to me

The alert condition for 'Malicous' was triggered.

Alert: Malicous
Search String: index=squid_access [| inputlookup phishtank.csv | rename url as uri | fields uri]
Trigger: Saved Search [Malicous]: always
Trigger Time: 03:04:13 on November 18, 2014.

View results in Splunk

_raw	_time	host	index	linecount	source
1416301451.113 0 64.131.110.223 TCP_MISS/304 403 GET http://creditihabbogratuiti.blogspot.com/ - HIER_DIRECT/173.194.46.107 -	Tue Nov 18 03:04:11 2014	64.131.110.126	squid_access	1	/var/log/squid/access.log

Figura 31: Email enviado al administrador.

La Figura 32 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.

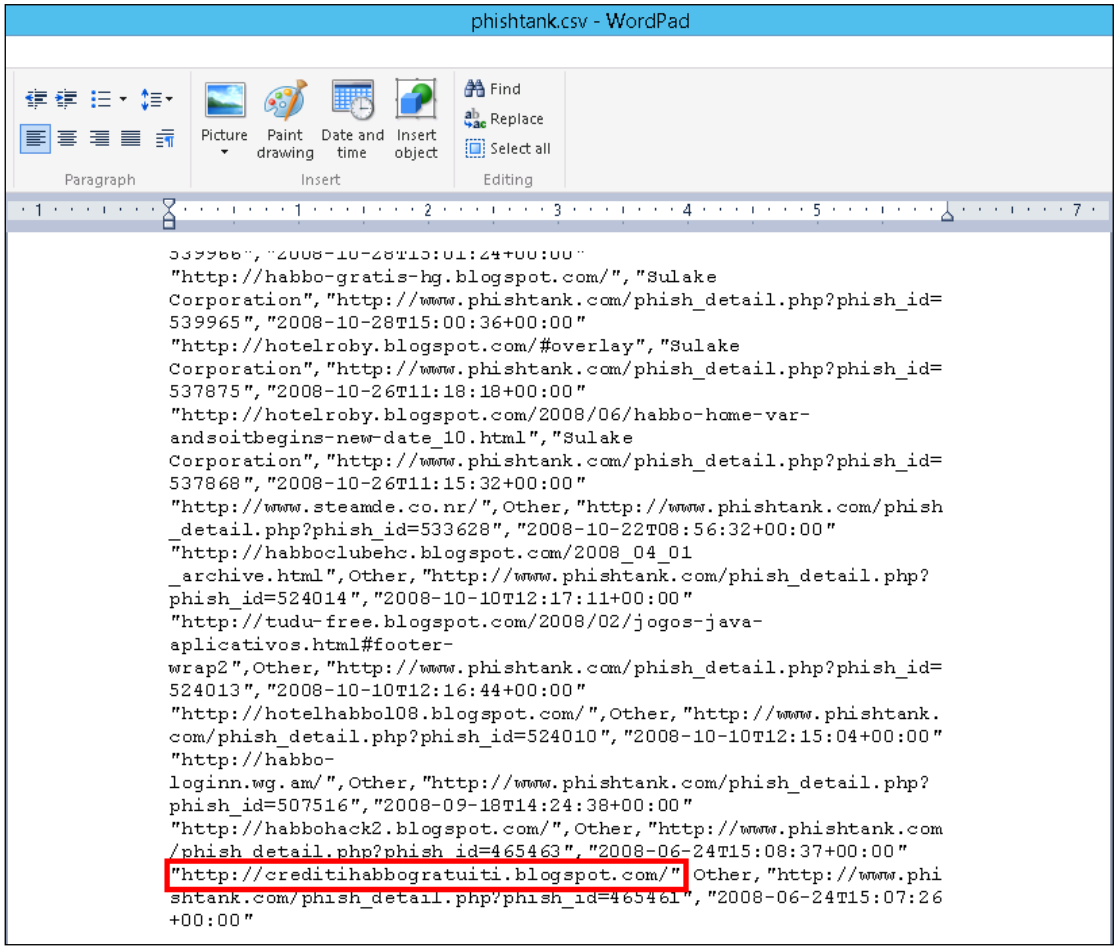


Figura 32: Archivo Phistank.csv (watchlist).

En este proyecto solamente se está 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.

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 permite 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

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

Baluja-García, W., & Anías-Calderón, C. (2006). Amenazas y defensas de seguridad en las redes de próxima generación. *Ingeniería y Competitividad*, pp. 7-16.

Durán, F. F., Mondragón M., N., & Sánchez M., M. (2008). Redes cableadas e inalámbricas para transmisión de datos. *Científica*, pp. 113-118.

Dussan Clavijo, C. A. (2006). informática. *Entramado*, pp. 86-92.

ESPINAL, A. A., MONTOYA, R. A., & ARENAS, J. A. (2010). GESTIÓN DE ALMACENES Y TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC). *estudios gerenciales*, p.p.28.

Herrera Burgos, R. (2012). Implementación de aplicaciones Informáticas basadas en Software Libre en Bibliotecas y Unidades de Información. *Revista e-Ciencias de la Información*, pp. 1-13.

Jacovkis, P. M. (2011). Las TIC en América Latina: historia e impacto social. *Revista Iberoamericana de Ciencia, Tecnología y Sociedad - CTS*, p.p.3.

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

M, J. V. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica*, vol.24 no.50.

Melo, A. H. (2008). EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001. *Revista de Derecho*, no.29.

PhishTank Org., What is PhishTank? From :https://www.phishtank.com/index.php

Salvadori, I. (2013). La regulación de los daños informáticos en el código penal italiano. *Universitat Oberta de Catalunya*, 19.

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

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

Splunk Inc.. Getwatclist Overview. From: https://apps.splunk.com/app/635/

Splunk Inc., Splunk Doc--Configure CSV and external lookups, From : http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Addfieldsfromexternaldatasources

Squid Org., Squid: Optimizing Web Delivery, From: http://www.squid-cache.org/