Trabajo fin de Grado en

Ingeniería de las Tecnologías de Telecomunicación

Protocolo de gestión de vulnerabilidades

Autora: María González Rodríguez

Tutora: Isabel Román Martínez

Departamento de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2019

Trabajo fin de grado
Ingeniería de Telecomunicación

Protocolo de gestión de vulnerabilidades

Autora:
María González Rodríguez

Tutora:
Isabel Román Martínez
Profesora colaboradora

Departamento de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2019

Trabajo fin de grado: Protocolo de gestión de vulnerabilidades

Autora: María González Rodríguez

Tutora: Isabel Román Martínez

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2019

El secretario del Tribunal

A mi familia

A mi tutora

Y al amor de mi vida

AGRADECIMIENTOS

La lista de personas a la que agradecer este proyecto es mas bien larga, dado que tengo muchísima gente que me ha ayudado, sobre todo con el apoyo moral, a lo largo de la carrera, por lo que intentaré ser breve.

- A mi tutora, por supuesto, que me ha aguantado tutorías y revisiones miles.
- A mi familia, tanto de sangre como política, por estar siempre a mi lado.
- A Alejandro, por creer en mí más que yo misma.
- A Mariluz, sin la que no estaría en este punto hoy.
- Y finalmente, pero no menos importante, a mis compañeros de Deloitte, sobre todo a Juan, por aportarme sus conocimientos.

He conseguido acabar esto por vosotros. Muchísimas gracias a todos.

RESUMEN

En este documento vamos a desarrollar un procedimiento para la gestión (análisis y prevención) de las vulnerabilidades que tienen los dispositivos de una red.

Usaremos Nessus para realizar un escaneo de la red y de los distintos dispositivos que se encuentran en esta según la IP asociada a estos.

Una vez tengamos el análisis de la red y en función de las vulnerabilidades encontradas, intentaremos mitigar las vulnerabilidades de los dispositivos de los que sea posible y a su vez iremos detallando los casos de uso de las posibles alertas de las que queremos ser notificados

Usaremos Splunk para analizar toda la información de la red y para correlar eventos, de tal forma que según el tráfico de la red y los logs que recibamos de los dispositivos, salten alertas de seguridad que recibiremos mediante correo electrónico.

Splunk nos servirá para sacar datos del tráfico y estadísticas de la red ya que es una poderosa herramienta de análisis de datos que nos permitirá comprender en tiempo real lo que está sucediendo en los sistemas de TI y en la infraestructura tecnológica de la empresa.

Una vez realizado todo el despliegue detallaremos como podría evolucionar este proyecto a la vez que evoluciona la red del cliente.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

VOCABULARIO

Red de Ordenadores	Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios. **[1]**
Seguridad Informática	Conocida como ciberseguridad, es la parte de las ciencias de las tecnologías de la información que se encarga de la protección de los datos que se encuentran en un ordenador o en una red de ordenadores**.** [2]
Vulnerabilidad	Es una debilidad o fallo en un sistema de información.
Amenaza	Toda acción que aprovecha una vulnerabilidad [3]
"Hacker"	Es alguien que descubre las debilidades de un equipo o de una red informática. [4]
Ataque	También conocido como **ciberataque** es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático [5]
Registro o "*Log"*	Grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular [6]
Escáner de vulnerabilidades	Herramienta que nos ayuda a realizar un análisis de los dispositivos de una red de ordenadores y a identificar las distintas vulnerabilidades que se encuentren en el análisis de estos.
SIEM	Un Sistema de gestión eventos e información de seguridad (SIEM del inglés *security information and event management*) es un sistema que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad permitiéndonos un análisis en profundidad de la situación. [7]
Hacker de Sombrero Blanco	Es como se denomina a los expertos de seguridad que no atacan de forma maliciosa los equipos. Se dedican a descubrir las vulnerabilidades para resolverlas y mejorar los sistemas.
Equipo Rojo (Red Team)	Se define como equipo rojo a los grupos de hackers de sombrero blanco que se dedican a intentar "romper" los equipos o los sistemas de seguridad para comprobar su integridad.
Equipo Azul (Blue Team)	Al contrario que el equipo rojo, el equipo azul se encarga de intentar proteger los sistemas, creando barreras o aplicando parches de seguridad.
Certificado	Es un fichero electrónico firmado por una autoridad para verificar el contenido de un sitio o sistema. [8]
Norma o estándar.	Son documentos aprobados por un organismo nacional, regional o internacional de normalización reconocido en el que se especifican ciertas características, especificaciones y/o reglas que debe de cumplir en un procedimiento o herramienta especifica. [9]

1 INTRODUCCIÓN

No hay finales, sólo principios. Ahí tienes. Así de sencillo. Y también elegante, ¿verdad?

Ed Greenwwod

Elminster, La forja de un mago

En este apartado desarrollaremos la motivación para la realización de este trabajo, su propósito y los objetivos que se pretenden cumplir, así como la metodología, los medios y las tecnologías empleados durante su desarrollo.

1.1 Motivación

Ahora mismo, la ciberseguridad es una prioridad para las empresas.

Los datos se han convertido en uno de bienes más importantes para las empresas. Dada la transformación que se está llevando a cabo en nuestra sociedad, ahora mismo todos los datos se almacenan de forma digital: Bases de datos de clientes, libros de cuentas, proyectos, presupuestos, datos de trabajadores…

Dado esto los ciberdelincuentes han encontrado cada vez más formas de acceder a los datos o de dejar a las empresas sin poder tener acceso a estos: los secuestros de datos mediante programas maliciosos como los *ramsonwares,* para luego pedir un rescate a cambio de devolver la información, la suplantación de identidades, los accesos remotos no deseados y los ataques de denegación de servicio son algunas de las técnicas más usadas con estos propósitos.

Por esto mismo, tener en cuenta las vulnerabilidades que tienen los sistemas de la empresa, así como un sistema de alertas de seguridad para detectar eventos anómalos en nuestra red y evitar ataques es algo hoy día imprescindible. Sin un buen sistema de seguridad podemos vernos o bien violando gravemente las leyes de protección de datos y causando un perjuicio a nuestros clientes o aún peor, perdiendo toda la información de la empresa.

Por todo esto en este proyecto se va a detallar un protocolo de actuación ante las vulnerabilidades, detallando como encontrarlas y solventarlas.

1.2 Objetivos

El principal objetivo es la formalización de un procedimiento para la gestión de vulnerabilidades.

Este procedimiento consta de 3 pasos principales, los cuales se detallarán más adelante.

→**Escaneo de Vulnerabilidades:** Realizaremos un escaneo de la red para encontrar las distintas vulnerabilidades de los equipos que queramos monitorizar posteriormente. Para realizar el escaneo utilizaremos la herramienta **Nessus Enterprise** la cual nos ofrece una gran variedad de posibilidades para realizar los escaneos de la red, desde centrarnos en equipos concretos (por IP) a subredes enteras, analizando todos los dispositivos que se encuentren en diferentes subredes con distintas configuraciones. Pueden realizarse en el momento o programarse, entre otras características que detallaremos más adelante.

→**Mitigación de las vulnerabilidades y creación de las alertas:** Dadas las vulnerabilidades que se encuentren una vez realizados los escaneos nos centraremos en:

- **Mitigar las vulnerabilidades:** Aplicando o bien las recomendaciones de Nessus o investigando los posibles parches o soluciones disponibles para solventar cada vulnerabilidad. También realizaremos los cambios necesarios en las configuraciones de los dispositivos analizados y de los servicios que se encuentran en estos que detectemos que son vulnerables.
- **Analizar cómo pueden ser explotadas** las vulnerabilidades que no podamos mitigar. Determinaremos casos de uso en los que definiremos qué tráfico podemos considerar malicioso. Esto nos servirá para crear alertas que nos adviertan respecto a este tráfico y así detectar posibles ataques.

→**Configuración del gestor de eventos e información de seguridad**: Un sistema de gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés) nos permitirá realizar el análisis de los datos de forma más sencilla. Además, con él podremos crear alertas de seguridad para los casos de uso que consideremos necesarios. En este caso hemos seleccionado como SIEM el software Splunk Enterprise.

Una vez configurado esto iremos importando los escaneos que realicemos para llevar una cuenta de las vulnerabilidades mitigadas y crear alertas en caso de que se detecten vulnerabilidades nuevas. Esto nos servirá para tener en cuenta las nuevas vulnerabilidades que puedan aparecer en los sistemas que estamos monitorizando.

Cuando tengamos el análisis de las vulnerabilidades buscaremos cuáles son una amenaza real para nuestro sistema. En este proceso realizaremos una búsqueda proactiva e iterativa a través de la red para detectar y aislar amenazas que evaden las soluciones de seguridad existentes.

Después procederemos a configurar los dispositivos para que envíen la información de sus registros al gestor principal, que será el que realice el indexado de los datos de toda la red. A estos dispositivos los llamamos "Forwarders". Estos son las instancias de Splunk que monitorizan eventos o estados de los dispositivos y mandan la información al Splunk Principal. Gracias a esto podremos monitorizar el estado de toda la red y generar las alertas previamente mencionadas, relacionadas tanto con un único host como con eventos correlacionados en la red.

Finalmente materializaremos este procedimiento en un caso de uso en concreto con Nessus y Splunk como hemos mencionado arriba. Como caso de uso hemos seleccionado la detección de un ataque mediante la técnica de desplazamiento lateral (también conocido como *pivoting* [10] [11]*)*, dado que es uno de los principales ataques que se efectúan hoy en día. Este ataque consiste en que un atacante, una vez que consigue introducirse en la red, intenta expandirse en ella y tomar el control de los máximos dispositivos posibles. Detallaremos el porqué de esta elección y como corregirla a lo largo del desarrollo del proyecto.

1.3 Metodología, Medios y Tecnologías.

Antes de comenzar a detallar el procedimiento que se ha seguido para desarrollar el proyecto, se va a describir brevemente las tecnologías utilizadas para realizar los escaneos y la gestión de los logs:

1.3.1 Vulnerabilidades

Lo primero que debemos explicar es que es una vulnerabilidad.

En el contexto de este trabajo entendemos vulnerabilidades como los "fallos", ya sea de código o de configuración, que pueden ser explotados por un actor externo y le permiten realizar acciones para las que no está autorizado.

La gestión de vulnerabilidades es clave en la era digital. Hay que identificarlas, clasificarlas, mitigarlas y si es posible remediarlas.

Un fallo de este tipo no siempre implica un riesgo tecnológico: Hay errores que no tienen impacto real al no permitir que las acciones que realice el actor externo tengan un efecto malicioso en el sistema. Un defecto se convierte en vulnerabilidad si hace que el comportamiento del sistema sea tal que pueda ser aprovechado para romper la seguridad de este. Sin embargo, es importante tener identificados los errores dado que, aunque no sean explotables en el momento de su descubrimiento, sí que lo pueden ser posteriormente.

Las vulnerabilidades pasan por múltiples etapas en su ciclo de vida. Hay que destacar que estas etapas pueden ocurrir en un orden distinto al que detallaremos a continuación o incluso pueden ocurrir al mismo tiempo (el caso de que una vulnerabilidad sea introducida intencionadamente en un producto hace que los hitos de Nacimiento y Descubrimiento ocurran simultáneamente.) Las etapas más importantes por las que pasa una vulnerabilidad son:

- ➔ **Nacimiento**: Se introduce, ya sea por defectos de diseño, de desarrollo o incluso intencionadamente, un fallo en el producto. Estos defectos pueden convertirse en riesgos para la seguridad del producto o del sistema en el que se esté usando.
- ➔ **Descubrimiento**: Se tiene conocimiento de la existencia de la vulnerabilidad. A la persona que la encuentra la denominaremos *Descubridor*.
- ➔ **Comunicación**: La vulnerabilidad ya no es solo conocida por su descubridor, si no que se transmite la información sobre su existencia a otras personas. Este traspaso de conocimientos se puede realizar de manera *pública*, de tal forma que la vulnerabilidad se hace conocida para la comunidad en general, y pasa entonces por su fase de **publicitación** o de forma *privada*, normalmente entre *hackers*.
- ➔ **Automatización de la explotación:** Esto ocurre si salen herramientas que nos permitan explotar la vulnerabilidad de forma automática. A esta herramienta o script la denominamos *exploit.*
- ➔ **Corrección:** Se corrige la vulnerabilidad mediante una actualización del producto.
- ➔ **Muerte:** Ocurre cuando la cantidad de equipos afectados es insignificante, ya sea porque ha dejado de usarse el sistema o porque se ha sacado una corrección de este,

La búsqueda de vulnerabilidades es un negocio muy rentable ahora mismo, en dos vertientes:

→Los atacantes quieren aprovechar estas vulnerabilidades en su beneficio de forma ilegal, ya sea por explotarlas ellos mismos o bien vendiendo la información sobre esta o exploits que permitan explotarla. Aunque el principal motivo para esto es el económico, también nos encontramos con atacantes que pretenden obtener información o simplemente afectar a la compañía y provocarle un daño ya sea material o de reputación.

→La profesional, realizada por personas/equipos normalmente contratados que se dedican a la búsqueda de vulnerabilidades de forma legal, ya sea para la empresa desarrolladora, por parte de un tercero o de forma altruista (para que estas vulnerabilidades se publiciten o se corrijan). También suelen ser profesionales los equipos que se dedican a corregir vulnerabilidades y los proveedores de productos relacionados con la gestión de estas.

En esta última parte entraría nuestro proyecto, ya que nuestro objetivo es corregir las vulnerabilidades encontradas en los sistemas del cliente, así como remediarlas y mitigar su impacto en las actividades de este.

1.3.2 Nessus Professional

Nessus Professional es un software ofrecido por la empresa **Tenable** [12] que nos permite encontrar vulnerabilidades en diferentes dispositivos con una gran versatilidad a la hora de configurar los escaneos que realiza para identificarlas.

Lo hemos elegido sobre sus competidores ya que:

- **Es fácil de usar:** Simplemente hay que instalarlo y abrir el cliente web, no requiere de más configuración.
- **Versatilidad:** Nessus nos ofrece multitud de configuraciones a la hora de realizar los escaneos, entre las cuales destacamos:
  - **Posibilidad de programarlo:** Podemos realizar simplemente una vez el escaneo o programarlo para que se ejecute cuando nosotros queramos. Además, nos ofrece la posibilidad de cancelarlos o incluso pausarlos para luego continuar.
  - **Autentificación:** Con esta solución podemos simplemente introducir cual es la subred en la que queremos realizar el escaneo para realizarlo en todos los dispositivos o introducir distintas formas de autentificación ya sea para acceder a los dispositivos (credenciales de usuario de Windows, por ejemplo) o a los servicios que estos ofrecen (si tiene un servidor web, autentificación por HTTP, por ejemplo, cuando queremos acceder a la consola de configuración de un router.)
  - **Historial:** Podemos ver el registro de los escaneos realizados y la información encontrada en ellos, incluso realizar informes de las diferencias entre ellos, lo cual nos facilitará la tarea de solventar las distintas vulnerabilidades.
  - **Diferentes tipos de escaneo:** Podemos hacer multitud de escaneos distintos, incluidos escaneos en servicios *cloud* y auditorias para la configuración de los dispositivos de la nube.

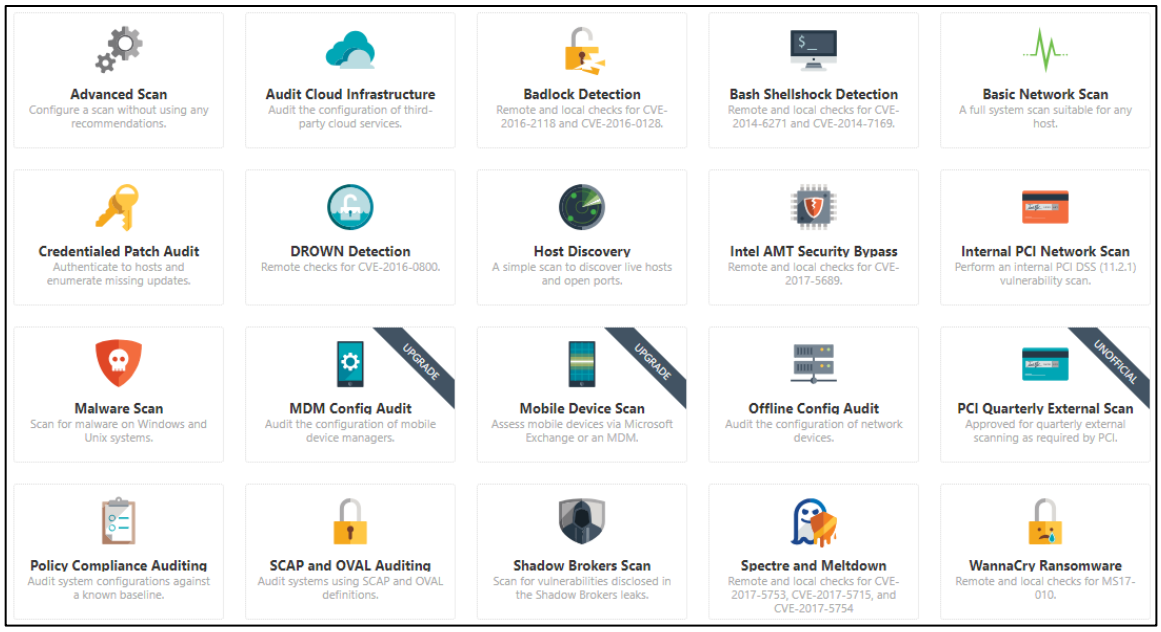
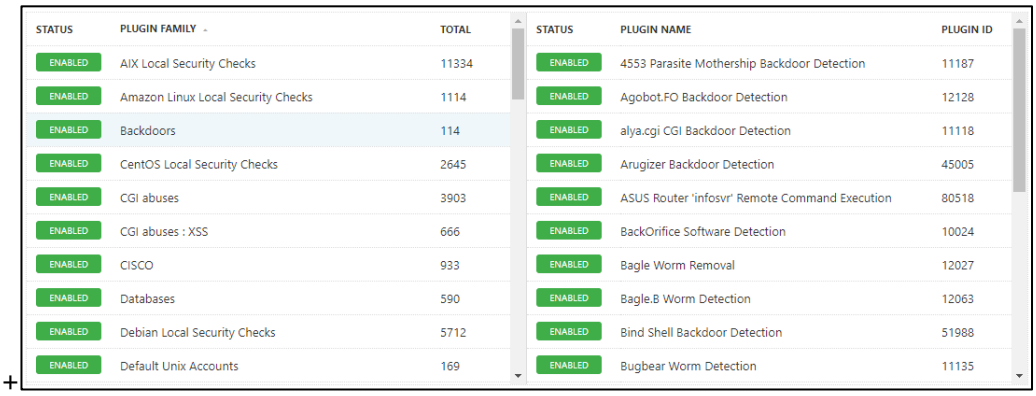


Ilustración 1: Diferentes tipos de escaneos

- **Se pueden seleccionar específicamente los plugins a la hora de realizar escaneos:** Nessus tiene multitud de plugins que nos dan integración con múltiples softwares y herramientas, pero para acelerar los escaneos podemos deshabilitarlos si no los necesitamos.



STATUS	PLUGIN FAMILY	TOTAL
ENABLED	AIX Local Security Checks	11334
ENABLED	Amazon Linux Local Security Checks	1114
ENABLED	Backdoors	114
ENABLED	CentOS Local Security Checks	2645
ENABLED	CGI abuses	3903
ENABLED	CGI abuses : XSS	666
ENABLED	CISCO	933
ENABLED	Databases	590
ENABLED	Debian Local Security Checks	5712
ENABLED	Default Unix Accounts	169

STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	4553 Parasite Mothership Backdoor Detection	11187
ENABLED	Agobot.FO Backdoor Detection	12128
ENABLED	alya.cgi CGI Backdoor Detection	11118
ENABLED	Arugizer Backdoor Detection	45005
ENABLED	ASUS Router 'infosvr' Remote Command Execution	80518
ENABLED	BackOrifice Software Detection	10024
ENABLED	Bagle Worm Removal	12027
ENABLED	Bagle.B Worm Detection	12063
ENABLED	Bind Shell Backdoor Detection	51988
ENABLED	Bugbear Worm Detection	11135

Ilustración 2: Plugins de Nessus para buscar vulnerabilidades especificas

- **Nos permite escanear diferentes tipos de vulnerabilidades:** como son las de acceso remoto, configuraciones que pueden afectar a la seguridad, puede detectar contraseñas por defecto o dispositivos que puedan provocar una fuga de información al recibir paquetes con valores inválidos que fuercen un comportamiento inadecuado.

➔ **Tiene integración con el SIEM que hemos elegido**: La selección de los programas que vamos a usar se detallará más adelante, pero uno de los motivos por el que hemos elegido estos dos programas es porque mediante las aplicaciones que Splunk (el SIEM que usaremos) nos proporciona podemos recoger fácilmente los datos registrados por los escaneos de Nessus.

➔ **Es rápido sin afectar a la red:** Aunque Nessus ofrece uno de los escaneos más rápidos de redes frente a sus competidores y es muy eficiente en cuanto a la gestión de recursos por sí solo, también se puede configurar el tráfico que va a usa y hacer que su funcionamiento se ralentice si esto llega a afectar a la red o a otros dispositivos.

➔ **Múltiples formas de exportar los datos**: Aparte de la compatibilidad con Splunk, Nessus nos ofrece múltiples formas de visualizar los datos de los escaneos y la información que queremos sacar de estos: desde una simple lista en CSV a un completo informe de las vulnerabilidades, su criticidad y a que dispositivos afecta.

Si simplemente queremos un análisis genérico, debemos seleccionar la opción "Basic Network Scan" en el menú de selección y se procederá a realizar un escaneo completo apto para cualquier host en el que lo único que tendremos que hacer es indicar la dirección IP del dispositivo a escanear.

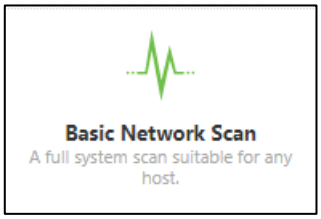


Ilustración 3: Escáner básico

1.3.3 Puerta trasera

Una puerta trasera es un método, habitualmente secreto, usado normalmente como acceso seguro a un dispositivo, para tareas de mantenimiento o actualizaciones.

Los fallos de seguridad pueden permitir utilizar una puerta trasera en ciertas aplicaciones o sistemas en el beneficio de los atacantes, que pueden usarlos para actividades maliciosas, por lo que es necesario que estén protegidos.

Cuando hemos realizado el análisis de vulnerabilidades hemos detectado no uno si no varios puertos abiertos sin autentificación en los servicios ofrecidos por la empresa, por lo que hemos decidido que sea esta la vulnerabilidad a estudiar en el caso de uso, dado que tiene una prioridad crítica.

1.3.4 Splunk

Splunk es una solución que nos ayudará a indexar, agregar y analizar la información recogida desde nuestra red, ya sea de los dispositivos internos o del tráfico que pueda provenir de fuera.

Dada su posibilidad de ***agregar*** eventos, es decir, unificar los eventos que sean del mismo tipo y con campos iguales, y también de ***indexarlos***, unificándolos en un *índice.* Esto nos permite almacenar los datos procesados para facilitar después la búsqueda de patrones entre la información que recolectamos, Splunk se ha convertido hoy en día en uno de los softwares más potentes de análisis de datos a gran escala o "big data".

Hemos escogido **Splunk Enterprise** para nuestro proyecto por múltiples razones que se basan en la información de la ilustración 4:

Ilustración 4: Cuadrante de Gartner sobre los SIEM

Gartner [13]es una empresa consultora que se dedica a la investigación de las nuevas tecnologías y que puntúa a las empresas según la habilidad de ejecutar con éxito su visión del mercado y el conocimiento de los proveedores para aprovechar el mercado. Clasifica a las empresas según 4 categorías: Lideres, aspirantes, visionarios y nicho de mercado dentro de su sector [14].

Como podemos ver, Splunk está situado entre los líderes de los SIEM según Gartner. [15]

Entre las principales características que hacen líder a Splunk encontramos:

- **Soporte**: Tiene una amplia documentación, así como un foro de preguntas propio, en el cual podremos encontrar solución a la mayoría de los problemas que puedan surgir dado el amplio uso de Splunk, no solo como gestor de alertas, también es un gran aliado a la hora de analizar un gran volumen de datos. Sus *dashboards* permiten mostrar los datos recolectados en multitud de formatos.

➔ **Rendimiento e integración**: Splunk nos permite medir los recursos que él está utilizando del sistema, así como el tráfico que está ocupando en la red.

Ilustración 5: Recursos usados por Splunk

Además, Splunk integra su propio gestor de logs. Tiene un índice interno en el que solo se indexan los logs relacionados con el funcionamiento de Splunk, lo que facilita la configuración y solucionar errores tanto a la hora de la configuración del Splunk principal como de las conexiones con los *forwarders*, cuyas características se detallarán más adelante.

➔ **Integración**: Splunk cuenta con una web en la que podemos encontrar aplicaciones desarrolladas para la integración de su sistema con multitud de dispositivos y aplicaciones, especialmente con dispositivos de seguridad de redes, ya que al fin y al cabo la función principal de este sistema es ser capaz de encontrar amenazas en nuestra red.

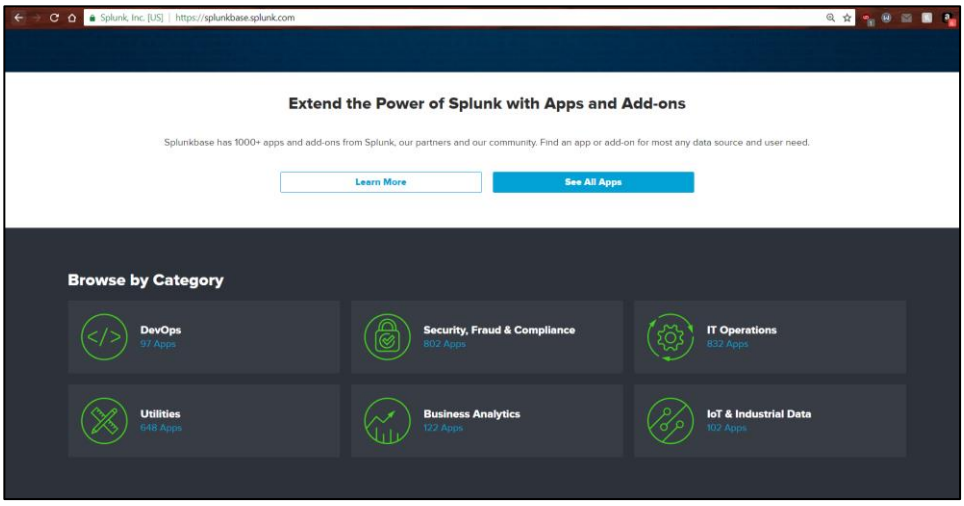


Ilustración 6: Splunk dispone de multitud de Apps

➔ **Capacidad de procesar los eventos en tiempo real**: Splunk es de los pocos gestores de datos que es capaz de recolectar y procesar los eventos en tiempo real, siempre dependiendo del retardo que pueda estar producido por la red. Dado que nuestro objetivo principal es la seguridad, esto hace que Splunk se convierta en uno de los mejores candidatos para gestionar los datos. Splunk está reconocido como el SIEM con mayor capacidad de búsqueda [16]

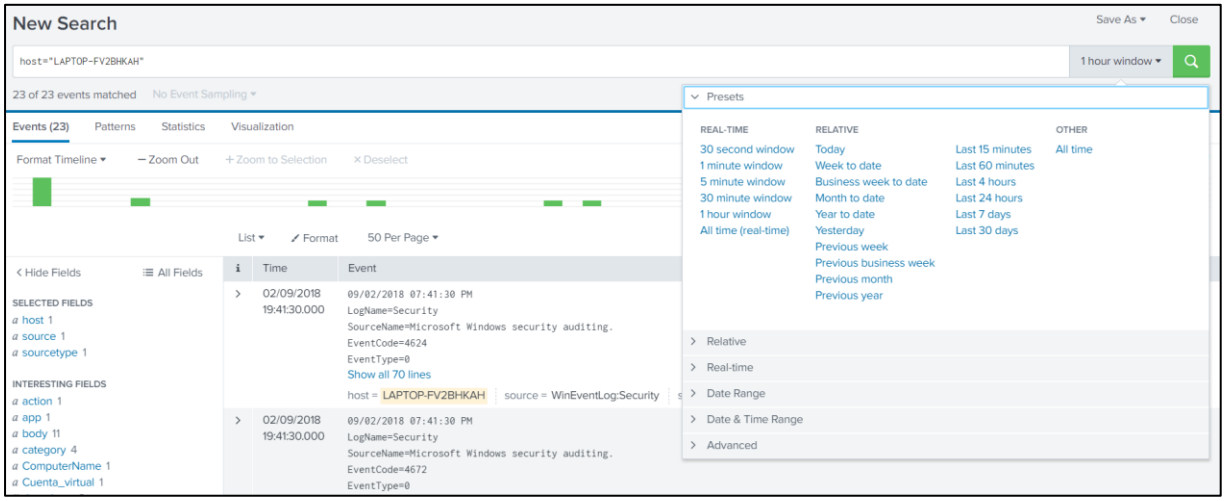


Ilustración 7: Búsquedas en tiempo real y gráfica de eventos

➔ **Escalabilidad**: Podemos elegir entre múltiples configuraciones tanto para instalar los recolectores de eventos, como a la hora de tratar los datos luego en función del volumen. Además, Splunk proporciona un servidor capaz de replicar la misma configuración en varios dispositivos, réplica de datos para tener tolerancia ante posibles fallos y balanceo de carga.

Dadas estas características, detallaremos la selección de estas tecnologías en los apartados siguientes.

1.3.5 Método de trabajo

A continuación, procedemos a detallar brevemente la metodología que se ha empleado para desarrollar el proyecto.

1. **Búsqueda de Información:** Antes de empezar a realizar nada se ha procedido a una búsqueda detallada de información sobre las herramientas a utilizar. Nos informamos de las distintas opciones que teníamos para implementar tanto el escaneo de la red como la gestión de eventos y comparamos las características que nos ofrecían. Finalmente, como hemos detallado arriba, nos decantamos por Nessus y Splunk, detallando el estado de la técnica y el porqué de esta elección en el siguiente capítulo.
2. **Definición de la arquitectura de la red:** En el desarrollo de este proyecto definiremos un protocolo de gestión de vulnerabilidades genérico, pero a la hora de implementarlo nos centraremos en el entorno de la pequeña empresa. En estos entornos nos encontramos por lo general con pocos equipos y en este caso nos vamos a centrar simplemente en 3 tipos:
    - **Maquinas con sistema operativo Ubuntu,** las cuales no disponen de interfaz gráfica por lo que deben ser configuradas mediante terminal. Son usadas por la empresa para su operativa diaria con diferentes servicios en diferentes puertos. En estos dispositivos nos centraremos en el servicio SSH que tienen habilitado para su mantenimiento y configuración.
    - **Los ordenadores de usuario**: portátiles con sistema operativo Windows 10, ordenadores plataformados con políticas de actualización de administrador y que no tienen posibilidad de personalización ni de instalación de programas fuera de la lista de software permitido.
    - **El router** que se usa como salida a Internet que es marca ZTE, al que dada su limitada configuración simplemente haremos un análisis de las vulnerabilidades.

    Los equipos Ubuntu incluyen numerosos servicios que son necesarios para el funcionamiento de la empresa. Como hemos comentado arriba, a la hora de realizar los escaneos nos hemos encontrado con que varios de esos servicios tienen su "puerta trasera" sin autentificación. Vamos a aprovechar esto para crear el caso de uso que vamos a manejar en el proyecto. Intentaremos detectar un ataque mediante la técnica de desplazamiento lateral, en el cual un atacante se aprovecha de este tipo de vulnerabilidades de autentificación para expandirse a través de la red. Estaremos buscando intentos de autentificación hacia los equipos vulnerables, ya que una vez que el atacante se encuentre dentro de cualquiera de nuestros dispositivos, intentará tomar el control de otros. Nos centraremos en las conexiones que usen el protocolo SSH dado que es el que más comúnmente se usa y es el que permite más control sobre la máquina hacia la que dirigimos el ataque.

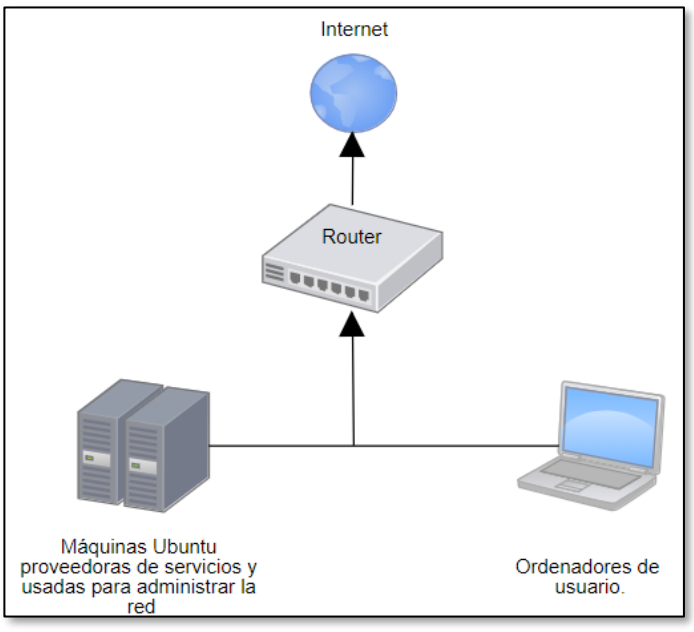


Ilustración 8: Esquema simple de la red

3. **Despliegue del SIEM:** Podríamos suponer que lo primero sería realizar un análisis de los equipos, pero, como hemos especificado arriba, desplegar primero el gestor de eventos nos ayudará a la hora de remediar las vulnerabilidades que puedan ser encontradas y nos avisará en caso de que puedan aparecer algunas nuevas, por lo que procederemos primero al despliegue del SIEM.

4. **Despliegue del escáner de vulnerabilidades:** La configuración del escáner en si no suele ser complicada, pero sí debemos configurar los distintos escaneos acordes a las características de nuestra red y seleccionar prudencialmente qué equipos vamos a examinar y cada cuánto.

   Para no sobrecargar la red innecesariamente deberemos configurar las distintas opciones y herramientas que nos ofrezca el escáner, como puede ser limitar el ancho de banda que usa la red o no activar las herramientas para equipos específicos, de los cuales no dispongamos en nuestra red.

5. **Realización de los escaneos:** Dada la topología de la red y de los equipos de esta, en este caso la realización de escaneos no supondrá una sobrecarga para la red ni afectará al rendimiento de los equipos, pero cuando nos encontramos ante redes grandes con multitud de dispositivos diferentes, esto puede llevar incluso días.

   Dependiendo de la magnitud de la red, el número de vulnerabilidades, la configuración que hayamos implementado y el impacto que queramos que tengan los escaneos en la calidad del servicio de la red deberemos programar estos escaneos para que se ejecuten en el momento adecuado, además deben repetirse de acuerdo con las políticas de actualizaciones de los equipos para ver qué vulnerabilidades se han solventado o si se han encontrado algunas nuevas.

   Realizaremos un escaneo sobre los distintos tipos de equipos de la red. Es importante ver las vulnerabilidades de todos los tipos de dispositivos ya que de por si una vulnerabilidad en un equipo no tiene por qué ser peligrosa, pero quizás si la unimos a alguna que tenga un equipo diferente la combinación de estas puede llegar a ser catastrófica si el atacante toma el control de varios dispositivos.

   Como hemos definido arriba nosotros tenemos: el router del sistema, el Windows que se instalará en los sistemas de los usuarios y la máquina Ubuntu que contiene los servicios de la empresa. Ya que los ordenadores de los usuarios son plataformados y con administración centralizada, nos bastará con realizar el escaneo de las vulnerabilidades y las actualizaciones que correspondan en un solo equipo para después exportar la nueva configuración a través de la red.

6. **Análisis de las vulnerabilidades encontradas:** Una vez obtengamos las distintas vulnerabilidades de los equipos procederemos a ver si pueden realmente afectar al desarrollo de la actividad de la empresa y si se pueden solventar o no.

   Es importante que el escáner que hallamos seleccionado por tanto tenga un histórico de las vulnerabilidades encontradas y sea capaz de sugerirnos formas de resolver los problemas que pueda encontrar.

7. **Monitorización de las vulnerabilidades de los equipos y seguimiento de los cambios en las configuraciones para mitigarlas:** Una vez acabado el análisis inicial deberemos llevar un seguimiento de las vulnerabilidades solventadas y las que aún permanecen en los equipos. Una vez registrada una vulnerabilidad en un equipo, aunque repitamos los análisis, esta no debe volver a registrarse, para evitar alertas innecesarias o posibles errores a la hora de actualizar o configurar los equipos.
   Realizaremos, como hemos mencionado arriba, escaneos periódicos sobre los equipos. Esto nos servirá tanto para ver si han surgido nuevas vulnerabilidades como para comprobar que efectivamente hemos corregido las vulnerabilidades una vez hemos realizado cambios en los equipos.

   Los datos sobre las vulnerabilidades de los equipos los deberemos almacenar directamente en nuestro SIEM, lo cual nos permitirá crear alertas en el caso de que se encuentren nuevas vulnerabilidades críticas en los sistemas.

8. **Creación de las alertas en función de las vulnerabilidades encontradas:** Una vez que tenemos la lista de las vulnerabilidades de los equipos podremos crear alertas en función de lo que queramos monitorizar y de los ataques que pueda sufrir la empresa.

   En la gestión de vulnerabilidades no nos podemos centrar solo en los equipos finales, también debemos intentar ver qué comportamientos o eventos pueden indicar un comportamiento maliciosos para intentar

implementar un sistema de alertas lo más efectivo posible. Nuestro objetivo será con esto la búsqueda de amenazas que puedan suponer un peligro real en la red y crear alertas en torno a ellas, intentando evitar el máximo posible de falsos positivos.

9. **Configuración de los equipos a monitorizar para que envíen logs:** Realizaremos la configuración del indexador de eventos en los dispositivos que queramos monitorizar.

   En el caso de Splunk nos ofrece 3 posibilidades de forwarders: El completo, el ligero y el universal [18].

   Aquí nos centraremos en dos:

   - **El complet**o para la gestión de los equipos de usuario, dado que nos dará más versatilidad a la hora de monitorizarlos y facilita la implementación de configuraciones personalizadas en caso de que fuera necesario. Si queremos monitorizar especialmente el pc de algún usuario o cambiar la configuración en función de la red o del trabajo que el usuario realiza solo debemos acceder a la consola web o editar los ficheros de configuración del equipo, lo cual nos ahorrará tiempo y nos facilitará enormemente la gestión.
   - **El universal**, ya que carga menos el sistema que el completo y es fácilmente configurable mediante ficheros y, al no disponer las máquinas de Ubuntu de interfaz gráfica, hace que este tipo de forwarder sea el ideal para utilizar en estos sistemas.

   Hemos descartado el uso del ligero ya que, aunque sigue estando disponible para su descarga, a partir de la versión 6.0 de Splunk se ha detenido su desarrollo.

10. **Visión de los datos y las alertas:** Se realizará un visionado de los datos que nos aporta la red a través de los distintos paneles de control de Splunk y de las alertas que hemos recibido a través del correo electrónico. A partir de las alertas podremos también ajustar las políticas de los escaneos que tenemos programados y la monitorización de los equipos.

Este método de trabajo es cíclico, es decir, se irá repitiendo, empezando desde el punto 5 hasta el 10, ya que tenemos que tener en cuenta los cambios que se produzcan en la red. Esto es un proceso que ha de repetirse para asegurarnos de que hemos asegurado nuestra red correctamente, así como para ajustar las alertas a las nuevas amenazas que puedan surgir.

Ilustración 9: Ciclo de la gestión de vulnerabilidades

11. **Evolutivo del proyecto con la red:** Debemos planificar cómo van a evolucionar las configuraciones de las herramientas de gestión que hemos decidido en función de cómo escale nuestra red cuando se incorporen nuevos equipos. Esto es importante sobre todo si tenemos un plan de ampliación, dado que quizás las características de las herramientas que hemos decidido no se adapten a la nueva red (número de equipos que nos permite escanear, volumen de tráfico que nos deja manejar, etc.)

2 ESTADO DE LA TÉCNICA

La descripción adecuada de una teoría debe ser lo más simple posible. Pero no demasiado simple

Albert Einstein

EN este capítulo explicaremos el contexto actual de las tecnologías y herramientas que hemos usado y que es lo que ha hecho que evolucionen hasta su estado actual, además explicaremos brevemente las características de cada una de ellas para conseguir que el lector se familiarice con ellas.

2.1 Contexto

En la actualidad casi todas las empresas y organizaciones reconocen la necesidad de hacer una transformación completa de la gestión de su información hacia la era digital que les permita desarrollarse y competir en el mercado.

A continuación, haremos una comparativa entre los escáneres de vulnerabilidades que se posicionan mejor actualmente, así como entre los SIEMs.

2.2 Escáneres de vulnerabilidades

Como se señaló anteriormente, lo primero que se debería realizar es un escáner de la red: ver qué problemas tiene y como solucionarlo.

Para ello usaremos un escáner de vulnerabilidades, herramienta que nos permitirá llevar a cabo una auditoría de nuestra red de forma automatizada, buscando vulnerabilidades y registrándolas según los parámetros que se ajusten a nuestras necesidades.

De nuevo, vamos a acudir a Gartner [19] para ver las diferencias entre los distintos escáneres.

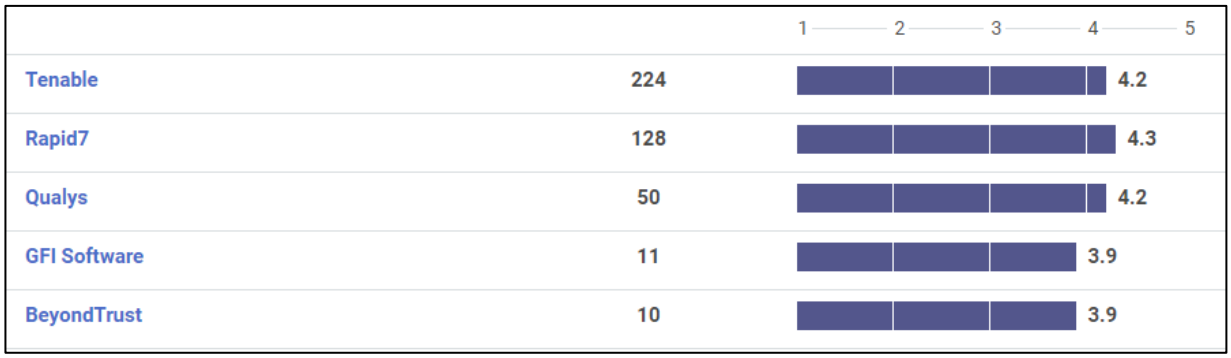


Ilustración 10: Calificaciones de las distintas empresas de escaneo

Y vamos a justificar nuestra elección dada la calificación de las empresas líderes en el sector. Nos centraremos en las 3 primeras, detallando brevemente sus características y comparándolas.

2.2.1 Qualys (Qualys)

Con Qualys nos encontramos con un escáner completo en todos los sentidos. Incluye integración con elementos en la nube, nos permite determinar qué aplicaciones se están ejecutando y en qué dispositivos de nuestra red en tiempo real y crear un mapa de nuestra red, entre otras múltiples características.

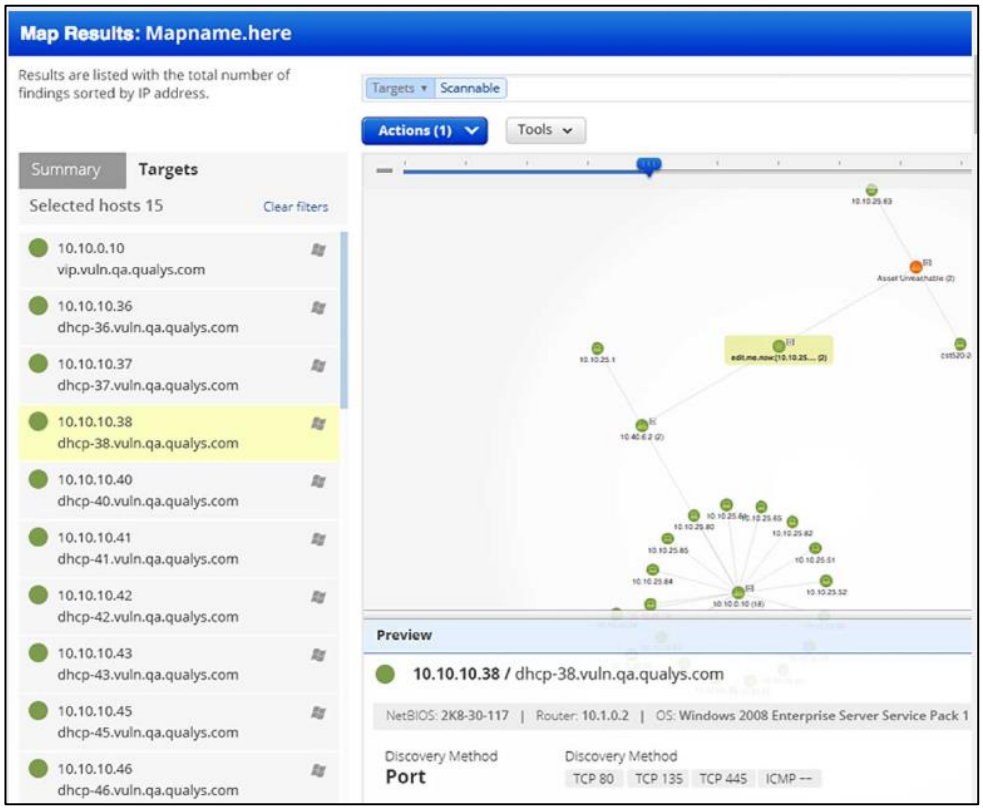


Ilustración 11: Mapa de red creado con Qualys

El único inconveniente que tiene Qualys y el por qué es menos usado con respecto a sus otros dos competidores principales, es la dificultad de configuración y despliegue dada la cantidad de herramientas que tiene.

Su uso tampoco es nada intuitivo, lo que hace que un usuario medio pueda encontrarse con grandes problemas para configurarlo además de que esto hace que la curva de aprendizaje sea mucho más lenta.

Ilustración 12: Experiencia del usuario. Ala izquierda Qualys y a la derecha Nessus

Dado todo lo anterior hemos decidido descartar Qualys como escáner a usar.

2.2.2 Nexpose (Rapid7)

De nuevo, al igual que con Qualys, nos encontramos con un software muy completo con gran cantidad de opciones de configuración y multitud de plugins y extras.

Dada esta cantidad de opciones, nos encontramos también ante un software tremendamente lento, que puede tardar hasta 10 veces más en realizar un escáner que sus competidores. Si bien ya trae preconfigurada varias políticas diferentes para la realización de escaneos, presenta muchas complicaciones a la hora de modificarlas, por lo que perderemos mucho tiempo en configurar las políticas antes de dar con la combinación ideal de permisos y restricciones.

También nos encontramos con una interfaz de usuario poco amigable y sin opciones de personalización, lo cual dificulta nuevamente la curva de aprendizaje y el tiempo de configuración.

Por último, hay que destacar que su precio es mucho mayor al de sus competidores, teniendo que pagar mensualmente por el tráfico que estimemos que vayamos a usar, y siendo la versión Enterprise (completa, para empresas) mucho más cara que la estándar.

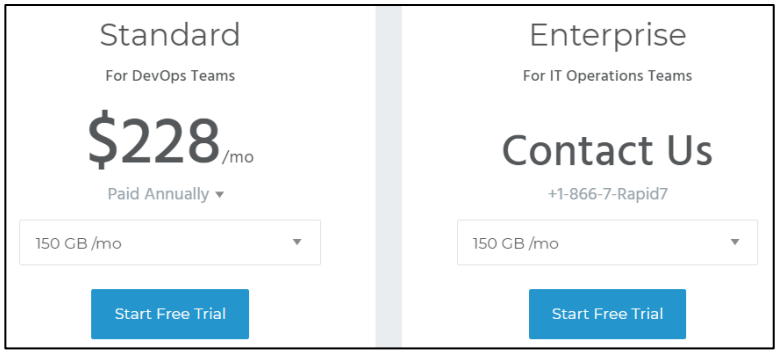


Ilustración 13: Precios de Nexpose

2.2.3 Nessus (Tenable)

Nessus es una potente aplicación de detección de vulnerabilidades perteneciente a la empresa Tenable, muy usada tanto por los hackers como por los expertos en seguridad informática cuando tienen que realizar auditorías.

Es una herramienta que detecta numerosos fallos de seguridad en base a plugins o módulos externos de pruebas que se van actualizando periódicamente.

Dado que es la que hemos seleccionado la describiremos con detalle más adelante, pero justificaremos su elección en el siguiente punto.

2.2.4 Software Libre

Aunque témenos varias alternativas interesantes de software libre como pueden ser **Nmap** [20], que es uno de los escáneres de puertos más usados, y las versiones gratuitas de algunos de los escáneres previamente mencionados, la verdad es que estas son muy limitadas, ya sea porque tienen unas características muy específicas y solo buscan vulnerabilidades concretas o por las limitaciones de recursos que tienen, ya sea poniendo un límite de IPs a escanear o de tráfico que pueden gestionar. Por tanto, no consideramos estas alternativas como una opción viable para la gestión de vulnerabilidades a gran escala como puede ser una empresa, que suelen tener múltiples equipos.

2.2.5 Comparativa

En la página web de Tenable podemos encontrar una comparación completa con otras soluciones del dominio de la gestión de vulnerabilidades [21] donde podemos ver sus múltiples beneficios frente a sus competidoras, pero debido a que esta podría ser una opinión sesgada vamos a recurrir también a la opinión de terceros.

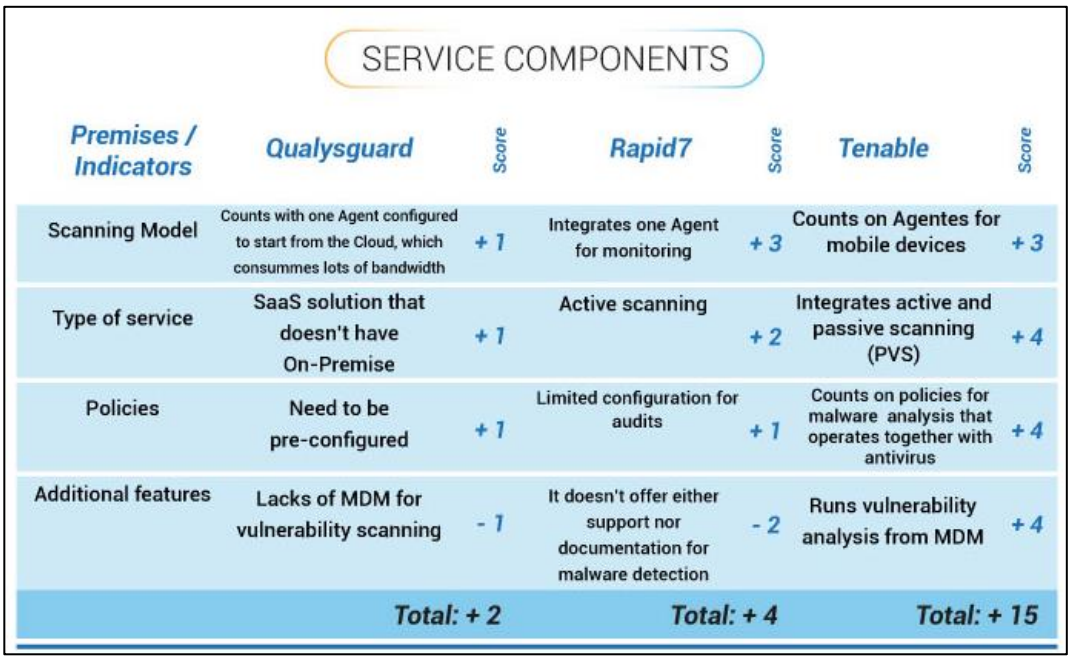
Como hemos podido ver en la ilustración 10, es una de las más usadas y con más reseñas positivas, dada la elevada media de su calificación con respecto a sus competidoras. Además, nos encontramos con que tiene más de un cuatro en todas sus características.

Ilustración 14: Calificaciones comparando distintas características de Tenable, Qualys y Rapid7

Lo que más cabe destacar de Nessus es su cómoda interfaz de usuario, la cual hace que la mayoría de los usuarios la recomienden frente a sus competidoras [22] , así como su casi nula interferencia con los sistemas sobre los que está trabajando.

Nessus no interfiere con los recursos de la máquina y, para evitar hacerla colapsar, incorpora agentes alojados en el servidor que hacen menos pesado el escáner, lo cual favorece la realización en paralelo de varios escaneos sin quitarle recursos al dispositivo. Tampoco interfiere con la red, ya que puede llegar incluso a parar el escáner si ve que esto afecta al rendimiento de ésta.

Lo hemos seleccionado también dado que la empresa desarrolladora (Tenable) está considerada como una de las mejores empresas para la gestión de la seguridad digital. Se lleva la mejor puntuación tanto en instalación como en interfaz de usuario y componentes. [23]



SERVICE COMPONENTS

Premises / Indicators	Qualysguard	Score	Rapid7	Score	Tenable	Score
Scanning Model	Counts with one Agent configured to start from the Cloud, which consummes lots of bandwidth	+ 1	Integrates one Agent for monitoring	+ 3	Counts on Agentes for mobile devices	+ 3
Type of service	SaaS solution that doesn't have On-Premise	+ 1	Active scanning	+ 2	Integrates active and passive scanning (PVS)	+ 4
Policies	Need to be pre-configured	+ 1	Limited configuration for audits	+ 1	Counts on policies for malware analysis that operates together with antivirus	+ 4
Additional features	Lacks of MDM for vulnerability scanning	- 1	It doesn't offer either support nor documentation for malware detection	- 2	Runs vulnerability analysis from MDM	+ 4
		Total: + 2		Total: + 4		Total: + 15

Ilustración 15: Comparación de los componentes de los servicios [23]

Añadiendo a todo esto su precio, mucho menor al de sus competidoras [24], y que además no nos pone límite ni de IPs ni de tráfico a los escaneos, hemos considerado que Nessus es la mejor opción para analizar los dispositivos de nuestra red.

2.3 Nessus

Más que un simple escáner, Nessus es una plataforma integrada que ofrece con la misma licencia la más extensa cobertura para la Gestión de Vulnerabilidades y verificación de configuraciones, plugins y actualizaciones de CVE y nos ayudará incluso a la hora de cumplir estándares de seguridad.

Lo primero que vamos a destacar es su precio con respecto a sus competidoras. Como ya hemos comentado antes, nos encontramos además con un precio fijo por licencia que no nos pone límites ni de tráfico, ni de IPs a escanear [25].

Nessus nos ofrece una gran versatilidad a la hora tanto de visualizar los datos como de exportarlos.

Con Nessus nos encontramos con una interfaz totalmente personalizable y atractiva, con un diseño intuitivo que nos permite ejecutar simplemente lo que necesitamos, sin necesidad de grandes configuraciones o cambios. Además, mientras se realizan los escaneos, podremos ver los resultados que se van encontrando en tiempo real, lo que acelera la detección y la priorización precisas de los problemas.

Gracias a los informes personalizables, podemos exportar la información que necesitamos sin ningún problema y con total facilidad, permitiéndonos esta herramienta incluso sacar comparativas entre varios escaneos en el formato que queramos (HTML, csv, nessus XML o pdf).

Gracias a todo esto, entre otras múltiples características que detallamos en apartados previos, Nessus se ha convertido en el escáner más usado en el mundo de la ciberseguridad y por ello lo hemos considerado como la mejor opción para este proyecto.

2.4 SIEMs

Características a tener en cuenta a la hora de seleccionar un siem [26]:

- **Gestor de Logs**: Dado que cada organización tiene una combinación única de logs, debemos asegurarnos de crear un listado de las posibles fuentes de logs de nuestra empresa y comparar esta lista con la de fuentes de logs compatibles del SIEM. Así nos garantizaremos un correcto funcionamiento de este y una correcta lectura de los datos por parte del SIEM.
- **Correlación de eventos:** La correlación de eventos es una de las herramientas más importantes que necesitamos en nuestro SIEM. Esta nos proporciona la capacidad de descubrir y aplicar asociaciones lógicas entre eventos individuales. Esta información nos permitirá una mejor toma de decisiones, identificar y responder a las amenazas de seguridad y validar la efectividad de los controles de seguridad.
- **Posibilidad de alertas de seguridad:** Los SIEMs nos dan la posibilidad de genera alertas cuando detecta actividad anómala. Debemos tener en cuenta las opciones que nos ofrecen a la hora de gestionar las alertas, así como la capacidad de estos para generar informes. También debemos tener en cuenta las opciones de respuesta que se nos ofrece ante estas alertas. Algunos SIEM pueden incluso actuar para bloquear actividades maliciosas, ejecutando scripts que activan la reconfiguración de los cortafuegos y otros controles de seguridad, por lo que esto será algo más a tener en cuenta.

Nos centraremos en los líderes según Gartner [27] como opciones entre las que elegir:

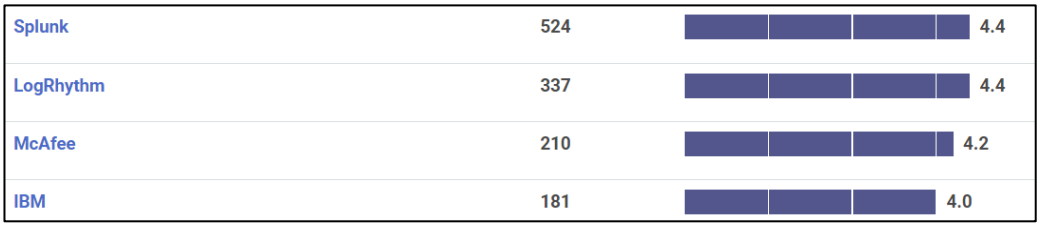


Ilustración 16: Valoración de los usuarios en Gartner

2.4.1 LogRhythm (LogRhythm SIEM)

LogRhythm se sitúa como líder en el cuadrante mágico de Gartner dada su gran cantidad de características y opciones de configuración. Sin embargo, esto hace que también sea uno de los más difíciles de desplegar y configurar.

Añadiéndole a esto su inexistente tienda de aplicaciones para facilitar su integración y su alto precio, hace que lo hayamos descartado como opción.

2.4.2 McAfee (Enterprise Security Manager)

Aunque McAfee se encuentra entre los SIEMS mejor valorados por los usuarios, su casi nulo despliegue en grandes empresas y, por tanto, la falta de documentación y su alto coste de procesamiento de datos, hacen que no sea rival frente a Splunk.

Ilustración 17:Comparativa de Splunk y McAfee [63]

2.4.3 IBM (Qradar)

A pesar de ser de los SIEMs más usados, vemos como Qradar está bastante por debajo de sus competidoras en cuanto a la calificación de los usuarios.
A pesar de ser un SIEM muy completo, su deficiente servicio al usuario y su alto coste (ni siquiera nos ofrece una versión de prueba gratuita) hacen que este SIEM quede relegado a un segundo plano en cuanto a sus competidoras, por lo cual lo hemos descartado.

2.4.4 Software Libre

Al contrario que en los escáneres, en el campo de los SIEMs nos encontramos con varias alternativas que son muy completas y que merecen mención:

- **Snort** [28]: Snort es un sistema de detección de intrusos en red (IDS), libre y gratuito. Implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación, provee de cientos de filtros o reglas para ataques de denegación de servicios entre otros. Sin embargo, el visionado de datos no es muy intuitivo, y encontrar los paquetes y la información de estos que coinciden con las reglas de detección establecidas, puede ser complicado. Por ello suele integrarse con SIEMs de mayor envergadura, que registran los logs de Splunk y nos permiten una visualización de los datos más sencilla.
- **ELK Stack:** Quizás la opción más destacable, compitiendo con las de pago, es este SIEM de la compañía Elastic. Este SIEM nos ofrecen un gran equipo de soporte, una gran integración con multitud de dispositivos y una gran facilidad para visualizar los datos. Sin embargo, se necesita un gran coste en infraestructuras para montarlo, así como su uso es mucho más complicado y su curva de aprendizaje más plana con respecto al resto, por lo que lo hemos descartado.

2.4.5 Comparativa

Podemos ver que, comparado con los otros líderes del mercado, Splunk destaca en algunas de las funciones que más vamos a usar, como en análisis de datos, en el manejo de logs y monitorización de usuarios [17].

Ilustración 18: Comparativa con otros de los líderes del mercado

Dado esto, y lo mencionado sobre sus competidoras en apartados anteriores, podemos entender por qué Splunk lidera el mercado, como podemos ver en la siguiente ilustración:

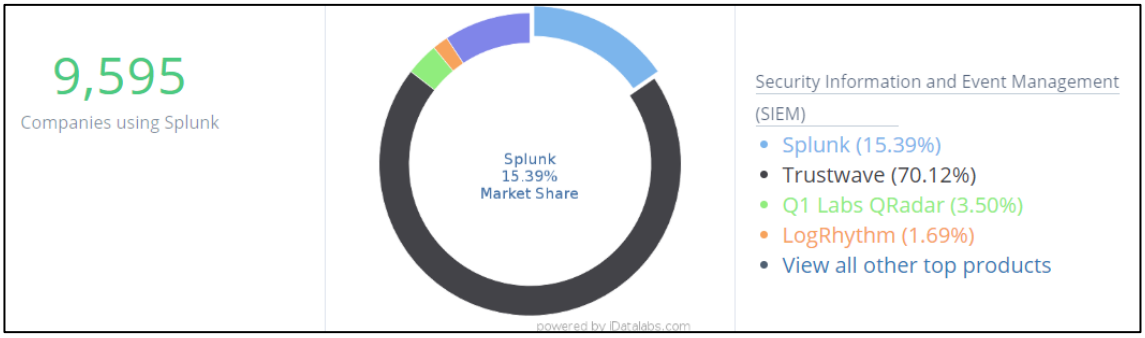


Ilustración 19: Compañías usando Splunk

No contamos *Trustwave* [28] ni lo hemos mencionado anteriormente dado que esta compañía se dedica a gestionar ellos la seguridad de otras compañías más pequeñas (Managed security service, MSSP [29]). Pero en este análisis [30] *SIEM* se trata como un servicio para la gestión de la seguridad, no solo como producto, por lo cual nos aparece en la gráfica.

Gracias a este liderazgo, Splunk cuenta con gran cantidad de documentación para su integración, dado que son los propios usuarios los que colaboran en esta en sus foros. Así mismo cuenta con herramientas para desarrollar aplicaciones que permiten la integración de múltiples dispositivos con su gestor de logs, y que están disponibles para los usuarios. Esto ha permitido que tengamos a nuestra disposición multitud de herramientas que nos facilitan la integración con nuestros sistemas.

Todo esto, junto sus múltiples características que se detallarán en los siguientes apartados, han hecho que elijamos Splunk como SIEM para nuestro proyecto.

2.5 Splunk

Una vez justificada nuestra elección de Splunk como SIEM para nuestro proyecto, al ser considerado uno de los líderes del mercado [31] y ser una de las elecciones de los consumidores de 2018 [32] , hablaremos de la empresa desarrolladora, así como de las características de la solución elegida, **Splunk Enterprise.**

2.5.1 Splunk Inc.

Splunk es una empresa desarrolladora de software fundada en 2003 con unos ingresos de 156 Millones y más de 600 empleados [33].

Sus soluciones se basan en buscar, monitorizar y analizar datos con el objetivo de hacerlos accesibles y permitirnos la identificación de patrones o el diagnóstico de problemas.

Nos ofrece licencias tanto gratuitas (diseñadas para uso personal) como de pago (para uso empresarial y en las que nos centraremos). Entre las características básicas de sus productos se incluyen: el indexado de datos, facilitarnos la búsqueda de éstos en los registros y en tiempo real, la posibilidad de reportar distintos casos de uso mediante alertas y la visibilidad de datos a través de paneles de estadísticas.

Sus productos principales son Splunk Light, Splunk Cloud y Splunk Enterprise, de los cuales hemos seleccionado Splunk Enterprise.

- **Splunk Light** [34]: Es una solución integral para entornos pequeños. Solo se puede usar un único servidor y no permite búsquedas distribuidas, a pesar de que sí tiene búsqueda y análisis de registros en tiempo real. A pesar de esto, esta solución se nos quedará pequeña cuando la empresa crezca. Dada estas y otras características, lo hemos descartado como opción.
- **Splunk Cloud** [35]: Es un "Software como servicio" o SaaS listo para la empresa. No requiere infraestructura, solo requiere configurarlo y se tendrán alertas con un retraso mínimo. Podremos tener un sistema híbrido de búsqueda integrando Enterprise con la solución Cloud. Sin embargo, este servicio es mucho más caro, por lo que nos hemos decantado por el Enterprise.
- **Splunk Enterprise** [36]: Splunk nos facilitará la recopilación, el análisis y el uso de los datos generados en las infraestructuras IT de nuestra empresa. Características como que no tenemos máximo de usuarios, ni de volumen indexado, así como que podemos tener todos los servidores que queramos, entre otras características que detallaremos más adelante, hemos decidido que esta es la mejor solución que podemos adoptar.

Features	Splunk Light	Splunk Enterprise
Maximum Daily Indexing Volume	20GB	Unlimited
Maximum Users	5	Unlimited
Universal Data Collection/ Indexing	•	•
Data Collection Add-Ons	•	•
Monitoring and Alerting	•	•
Dashboards and Reports	•	•
Search and Analysis	•	•
Automatic Data Enrichment	•	•
Anomaly Detection	•	•
Data Models and Pivot		•
Packaged Apps		•
Scalability	Single Server	Unlimited
High Availability		•
Disaster Recovery		•
Clustering		•
Distributed Search		•
Performance Acceleration		•
Access Control	User and Admin only	Granular and Customizable
Single Sign-On/LDAP		•
Developer Environment		Full access to APIs and SDKs
Support	Standard	Enterprise/Global

Ilustración 20: Principales diferencias entre Splunk Light y Enterprise

2.5.2 Características:

En Splunk tenemos:

- **Forwarders**: Los forwarders o "reenviadores" son instancias de Splunk que tienen la función de enviar los datos que deseamos monitorizar hacia el Splunk principal. Estos forwarders pueden reenviar la información de los dispositivos donde están instalados y que queremos monitorizar o pueden incluso reenviar información de otros equipos que le envían al forwarder información, quedando ese dispositivo con dos funciones, la de forwarder y la de *indexer*. Los forwarders pueden enviar la información a un solo indexador o a varios a la vez.

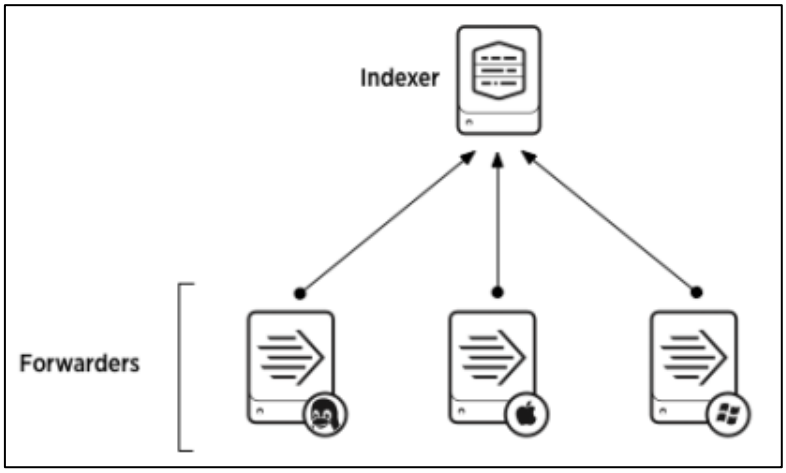


Ilustración 21: Arquitectura básica de una posible configuración con 1 indexador y 3 forwarders.

- **Deployment server:** Llamaremos Deployment server a la instancia de Splunk que centraliza el manejo de la configuración, agrupando y gestionando cualquier número de instancias de Splunk Enterprise. Dada esta característica de Splunk, lo hace ideal para gestionar las vulnerabilidades en las empresas, dado que lo normal es que tengan ordenadores plataformados a los que queremos aplicar la misma configuración.

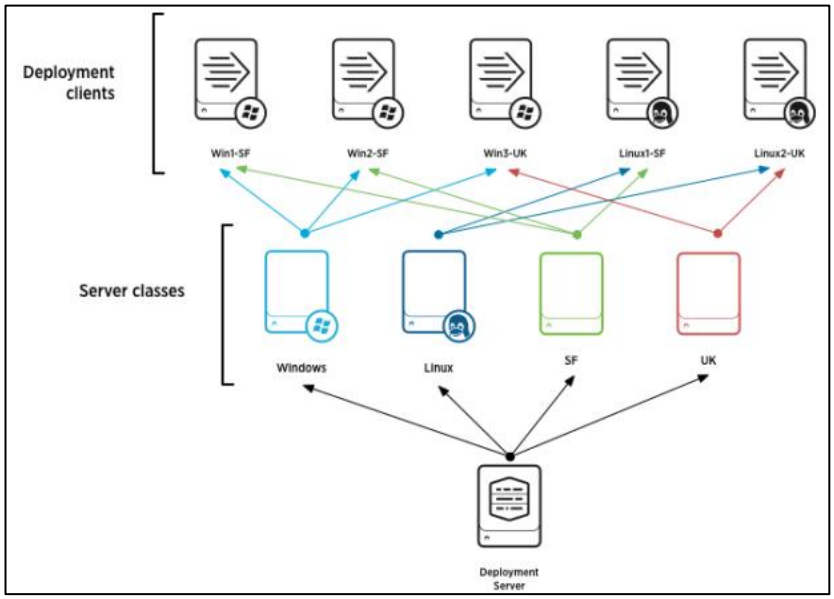


Ilustración 22: Arquitectura del Deployment Server [37]

Como podemos ver en la imagen, nos encontramos con que el Servidor tiene varias configuraciones distintas para los distintos sistemas operativos o los distintos servicios que se necesitan (las distintas "*Server classes*" que podemos ver en la imagen), cuyas características podremos exportar a los distintos clientes (*Deployment clients*) según las necesidades que tengamos. Con esto tendremos centralizada la configuración y podremos expandir los cambios por la red fácilmente.

Además, desplegar un cliente es muy sencillo, podemos hacerlo simplemente con un comando mediante CLI, lo cual minimizará la intervención del usuario.

```
msfadmin@metasploitable:/opt/splunkforwarder/bin$ sudo ./splunk set deploy-poll 192.168.1.134:8089
Your session is invalid.  Please login.
Splunk username: admin
Password:
Configuration updated.
msfadmin@metasploitable:/opt/splunkforwarder/bin$
```

Ilustración 23: Instalación de un cliente

Gracias a esto, Splunk nos permite ***[38] [39]***:

- **Crear alertas con información de toda la red*:*** Podremos crear múltiples alertas que incluyan información de varios dispositivos de la red.
- **Recoger e Indexar datos desde cualquier fuente y localización**, incluso importar los datos que ya hayamos recogido previamente. Podemos analizar y correlar datos sin las limitaciones que supondría una base de datos tradicional.
- **Hacer búsquedas, analizar datos y visualizar estadísticas fácilmente** gracias a su potente motor de búsquedas y la posibilidad de crear diferentes tableros de control (llamados Dashboards).
- **Monitorizar los datos de los equipos de la red y crear informes:** Podremos monitorizar equipos con configuraciones diferentes e incluso ver los datos en tiempo real y sacar informes de los datos conseguidos.

2.5.3 Arquitectura

Splunk nos hará de intermediario entre los empleados de la empresa encargados de la seguridad y los datos recolectados.

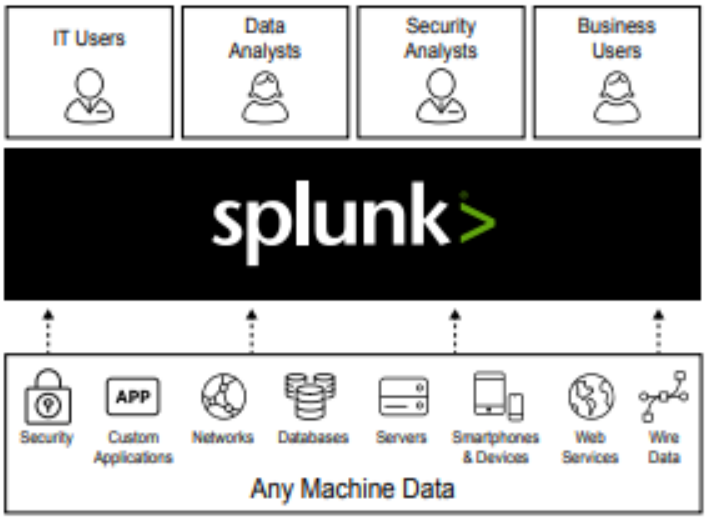


Ilustración 24: Estructura de Splunk

Dada su versatilidad y las múltiples posibilidades que nos ofrecen los forwarders, podemos configurar Splunk con múltiples arquitecturas. Esto es gracias a la diferenciación que hace Splunk de cada una de sus características y a las capas en las que se estructuran estas funcionalidades. Podemos ver en la siguiente figura como puede el usuario comunicarse con Splunk y las capas en las que se estructura éste.

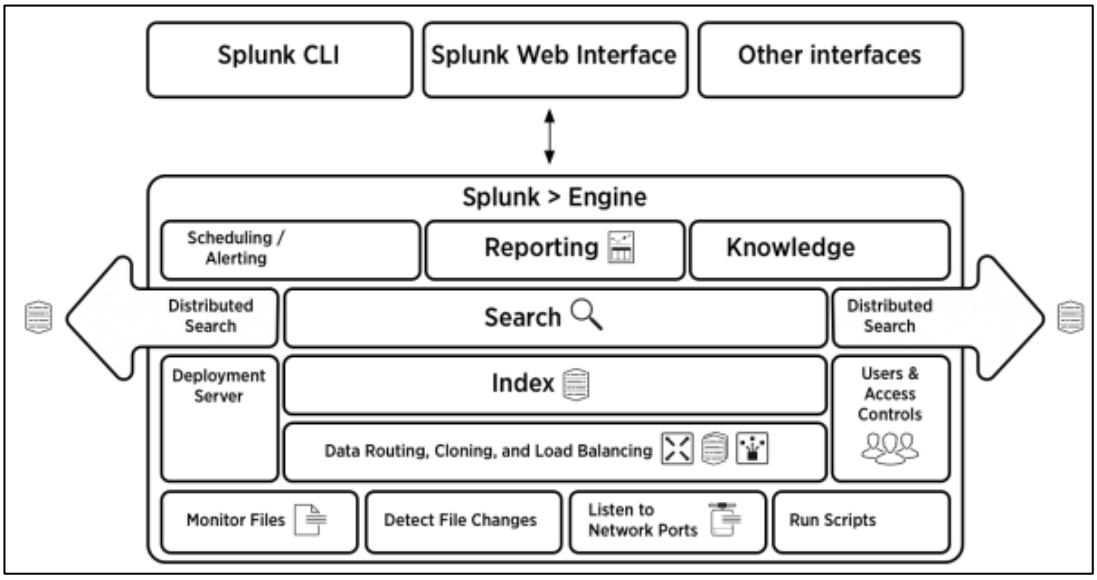


Ilustración 25: Diagrama de comunicación de Splunk con el usuario

Podemos dividir este diagrama en dos partes:

- Las funciones principales con las que manejaremos la información están situadas en el núcleo de Splunk y forman parte de su centro de procesamiento. Estas funciones son la de monitorización, indexado, búsqueda e informe.
- La interfaz de comunicación del usuario con el centro de procesamiento, la cual permite la configuración de éste y la visualización de los datos. Esta configuración puede realizarse mediante CLI[1], mediante la interfaz web o por otros medios.

Podemos configurar la arquitectura de Splunk todo lo sencilla o todo lo compleja que queramos, lo cual convierte a Splunk en una de las herramientas más versátiles para la gestión de logs y alertas. Gracias a que Splunk tiene sus funcionalidades muy bien definidas y separadas entre si (como vemos en la ilustración 19) y a que los forwarders pueden tener distintas configuraciones y podemos seleccionar qué datos de cada uno de ellos queremos monitorizar y hacia dónde queremos enviar esos datos para que se indexen, podremos configurar un balanceo de carga en nuestro sistema e incluso podremos reenviar los datos a varios indexadores para crear un sistema de soporte mediante redundancia [40] . Con todo esto conseguiremos un sistema robusto y con tolerancia a los fallos.

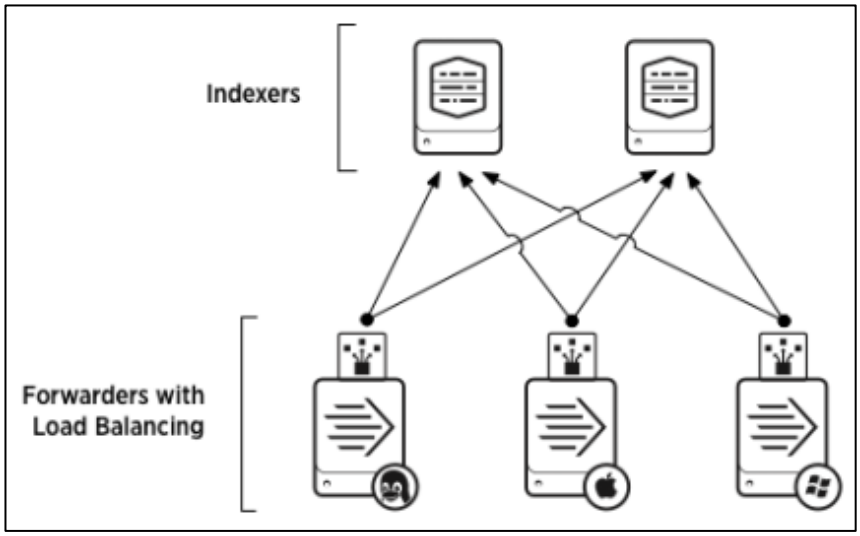


Ilustración 26: Arquitectura de múltiples forwarders con múltiples indexadores

[1] CLI: Estas siglas pertenecen al inglés Command Line Interface, es decir, interfaz de línea de comandos.

3 DESARROLLO DEL PROYECTO

Y el pensamiento es necesario ejercitarlo, se debe cada día y de nuevo y de nuevo pensar, para conservar la vida del pensamiento.

Gustavo Adolfo Bécquer

Detallaremos en este capítulo el proceso realizado para llevar a cabo el caso de uso específico que hemos seleccionado para este proyecto según la metodología que especificamos en el apartado 1.3.3.

Detallaremos también los problemas encontrados a lo largo del desarrollo del proyecto, así como los detalles de cómo solucionarlos.

Al final nos encontraremos con la siguiente configuración de los programas utilizados:

Ilustración 27: Instalación final de las herramientas

3.1 Despliegue del Indexador principal de Splunk

Como explicamos al principio de esta memoria lo primero que realizamos es el despliegue del Splunk principal, el que hará de receptor de todos los eventos e indexará los logs de todos los equipos.

De los productos para gestión de eventos ofrecidos por Splunk, nos quedaremos con **Splunk Enterprise,** la cual es su solución más usada. Splunk Enterprise nos ofrece una plataforma de inteligencia operacional que nos permite analizar con gran facilidad un gran volumen de datos.

Con esta solución tendremos un efectivo sistema de gestión e indexado de logs con el que podremos sacar información importante sobre la empresa, así como monitorizar los posibles riesgos de nuestra red, detectando ataques y amenazas.

Ilustración 28: Usos de Splunk

Lo primero que haremos será descargar Splunk de su página oficial. Splunk es un software comercial, pero tienen una licencia de 60 días para probarlo que nos permite indexar hasta 500Mb al día de datos. Usaremos esta prueba y la última versión para realizar este proyecto, aunque en el sector comercial hemos usado una versión de pago.

Ilustración 29: Descarga de Splunk

Nos lo encontramos disponible para Windows, Linux y Mac OS. En este caso el portátil del administrador es un sistema Windows, procederemos a su descarga e instalación. A lo largo de la descarga nos pedirá que introduzcamos una cuenta de administrador. Ponemos la que deseemos y finalizamos la instalación.

Una vez acabada, Splunk se instalará como un servicio disponible en nuestro sistema, cuyo comportamiento podremos configurar a nuestro gusto.

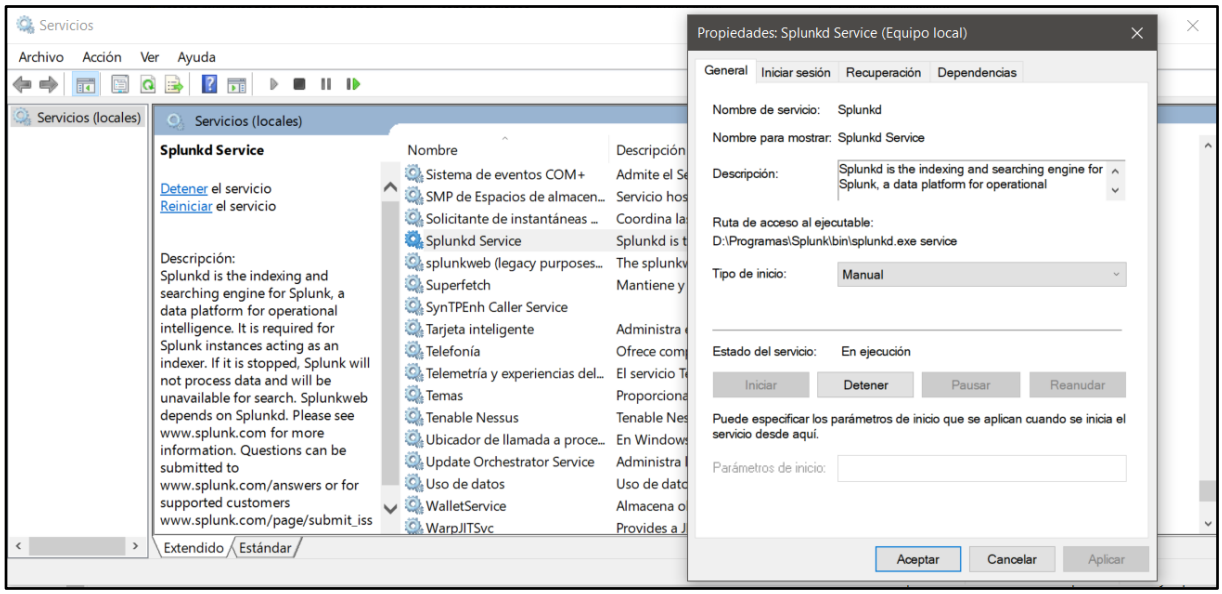


Ilustración 30: Splunk como servicio del sistema

En este caso gestionaremos Splunk a través de su interfaz web, disponible en el puerto 8000 por defecto y a la cual podremos acceder a través de cualquier navegador.

A partir de esta interfaz podremos acceder a la configuración completa de Splunk. Esta interfaz la tendremos disponible para los Splunk que ejercen como indexadores principales o para los forwarders completos, que se instalan mediante el mismo paquete, pero para los forwarders light o los universales no tendremos esta interfaz, por lo que las configuraciones las tendremos que realizar mediante ficheros de configuración o mediante comandos a través de terminal. Cuando realicemos esta configuración detallaremos qué información reenviamos y cómo lo hacemos al indexador principal.

Podremos acceder a la configuración mediante el usuario *admin* con la contraseña que hayamos seleccionado.

Ilustración 31: Pantalla de autentificación de Splunk

Una vez autentificados nos sale la pantalla principal de Splunk, que nos llevará a los menús principales.

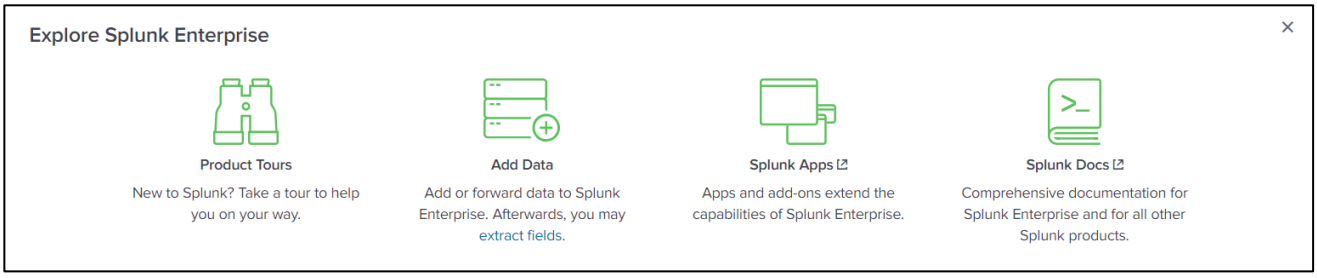


Ilustración 32: Posibilidades de inicio de Splunk

Splunk nos ofrece distintos "tours" por su aplicación para indicarnos donde están las funciones principales, sobre todo si es la primera vez que se usa. Cada vez que se visita una ventana por primera vez da la posibilidad de mostrar las funciones principales.

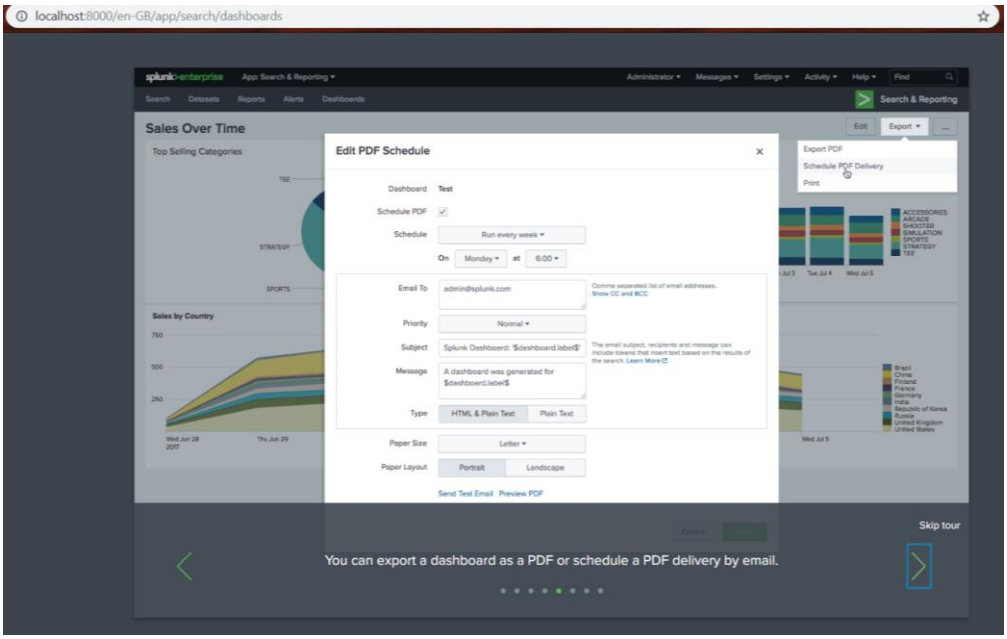


Ilustración 33: Ejemplo de tour por Splunk, en este caso de los dashboards

Vamos a empezar con la configuración como servidor del Splunk Principal. Estas opciones las encontraremos dentro del menu desplegable de la esquina superior izquierda.

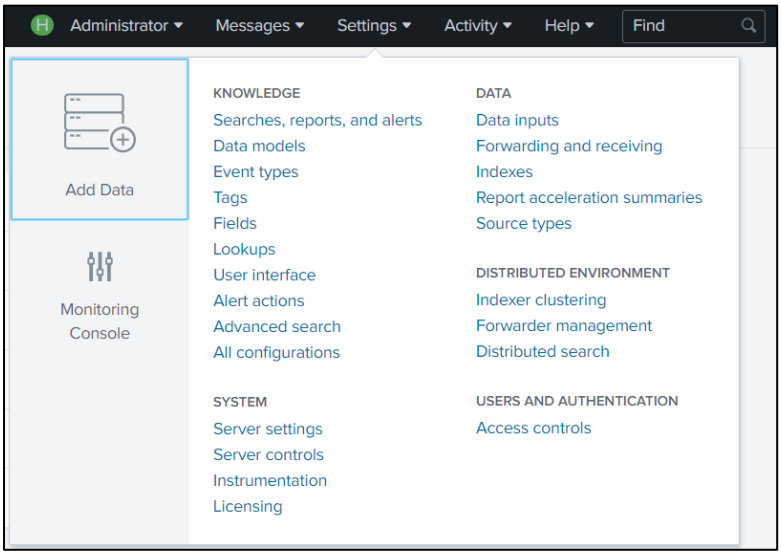


Ilustración 35: Configuración de Splunk como servidor

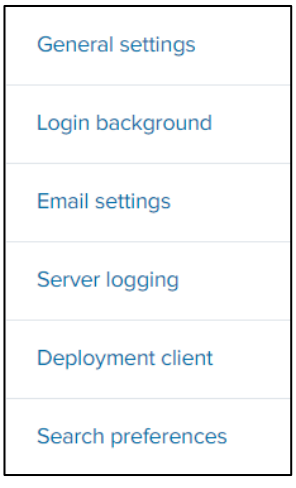


Ilustración 34: Menús de configuración

Cuando entramos en los menús de configuración veremos una pantalla acorde al menú en el que estamos navegando. En él encontraremos un formulario que podremos rellenar con los valores acordes a la configuración deseada.

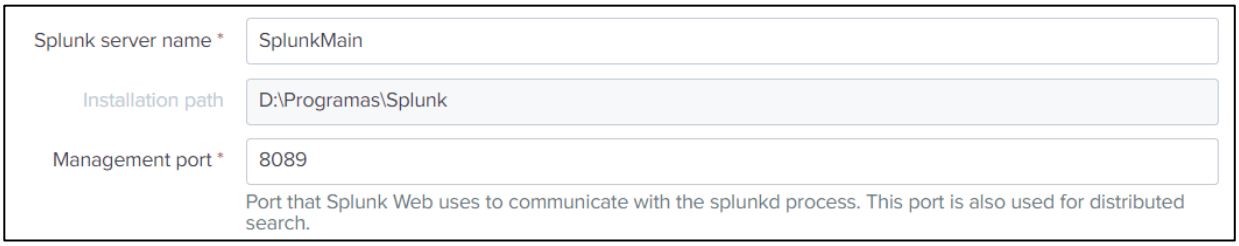


Ilustración 36: Ejemplo de formulario de configuración

Vamos a empezar por las configuraciones generales. Los valores que vamos a definir para nuestro proyecto son:

Tabla 1: Configuraciones generales de Splunk

VARIABLE	VALOR	DESCRIPCIÓN
SPLUNK SERVER NAME	SplunkMain	Nombre del servidor que nos servirá para identificarlo entre los despliegues de Splunk
MANAGEMENT PORT	8089	Puerto de escucha para los procesos de Splunk
RUN SPLUNK WEB	YES	Habilita la consola Web
WEB PORT	8000	Es el puerto donde la aplicación web está escuchando.
SESSION TIMEOUT	3h	Definimos el tiempo que estará abierta la sesión web

Esta ventana nos mostrará también la ruta donde hemos instalado el Splunk, nos da la posibilidad de habilitar https para el Splunk web, entre otras configuraciones.

Dado que vamos a usar Splunk para gestionar la seguridad de los sistemas, usaremos la posibilidad de mandar emails cuando se detectan alertas, cuya información gestionaremos posteriormente.

Para su envió configuraremos un servidor de correo.

Tabla 2: Configuración de Splunk para conectarse con el servidor de correo

VARIABLE	VALOR	DESCRIPCIÓN
MAIL HOST	smtp.gmail.com:587	Servidor que se va a usar. En este caso un correo de Gmail.
EMAIL SECURITY	Enable TLS	Método de autentificación
USERNAME	nuevaalertasplunk@gmail.com	Cuenta de correo que vamos a usar para mandar las alertas
CONTRASEÑA Y CONFIRMAR CONTRASEÑA	Introducimos la contraseña de la cuenta	Contraseña de la cuenta de gestión.

En esta pantalla de configuración también podremos configurar los aspectos visuales y de diseño de los emails que mandamos: la cabecera del correo, como se imprimen los informes en pdf, si se quiere incluir un logo, entre otras. Ahora mismo no nos vamos a centrar en el formato de los correos, pero es algo que podemos personalizar más adelante.

Como hemos podido ver en la imagen de arriba, tenemos muchas más funciones de personalización (eligiendo los logos para la pantalla de autentificación o configurando preferencias a la hora de hacer búsquedas) y configuración (como opciones de autentificación en el servidor) en Splunk, pero no serán necesarias en el alcance de nuestro proyecto.

Por último, tenemos que configurar el puerto de escucha para los eventos provenientes de los forwarders. En este puerto será donde recibamos todos los datos que estamos monitorizando en los distintos forwarders, a diferencia del 8089, configurado arriba, que es el de escucha para las configuraciones de Splunk. Para ello tendremos que definir un puerto que solo tenga este uso. En nuestro caso hemos decidido el puerto 9997, que es el que se usa de forma habitual con este propósito.

Para ello tendremos que ir de nuevo al menú superior, como mostramos en la parte de arriba, y seleccionamos Settings → Debajo del menú Data: **Forwarding and receiving**

Dentro de este menú podremos configurar todo lo relacionado con la recepción de logs en el Splunk principal y en el caso de que estuviéramos en un forwarder, la dirección del Splunk principal y la configuración de los datos que se mandan.

Como estamos configurando el Splunk principal, vamos a configurar la recepción de logs. Para ello nos vamos a Receive data → Configure receiving → Add new:

Ilustración 37: Menú para habilitar la recepción de datos

Una vez ahí nos aparecerá un formulario donde podremos rellenar el puerto para los logs.

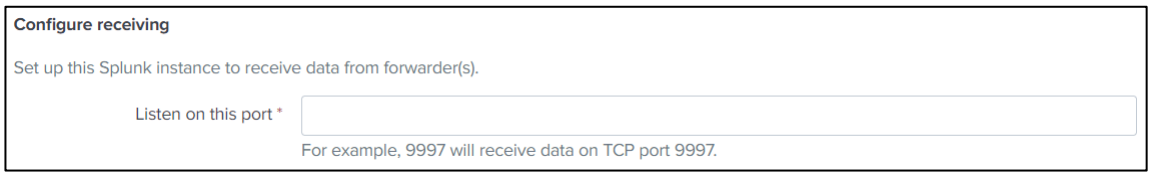


Ilustración 38: Formulario para añadir el puerto de escucha

Una vez añadido el puerto lo podremos ver en la lista de puertos de escucha.

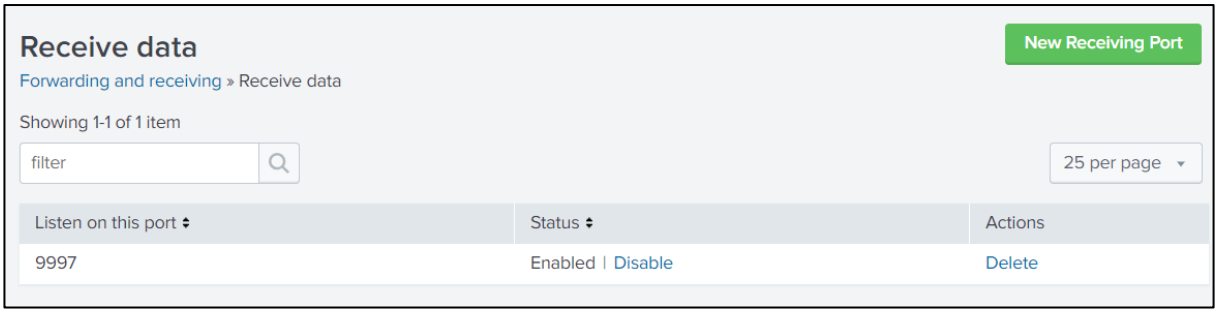


Ilustración 39: Puertos de recepción de eventos

Esta configuración la podemos realizar también por línea de comandos:

```
D:\Programas\Splunk\bin>splunk enable listen 9997 -auth admin:Alexia88

D:\Programas\Splunk\bin>
```

Ilustración 40: Habilitar el puerto de escucha por línea de comandos

Cabe mencionar que todos los puertos usados deben estar abiertos y debe haber conectividad entre el Splunk principal y los forwarders. Para ello debemos configurar correctamente el firewall de equipo que vaya a ocupar la función de *indexer*. Este ha sido uno de los problemas principales encontrados, ya que por defecto estos puertos suelen estar cerrados y muchas veces encontrábamos que no se recibían eventos y no encontrábamos el error de configuración.

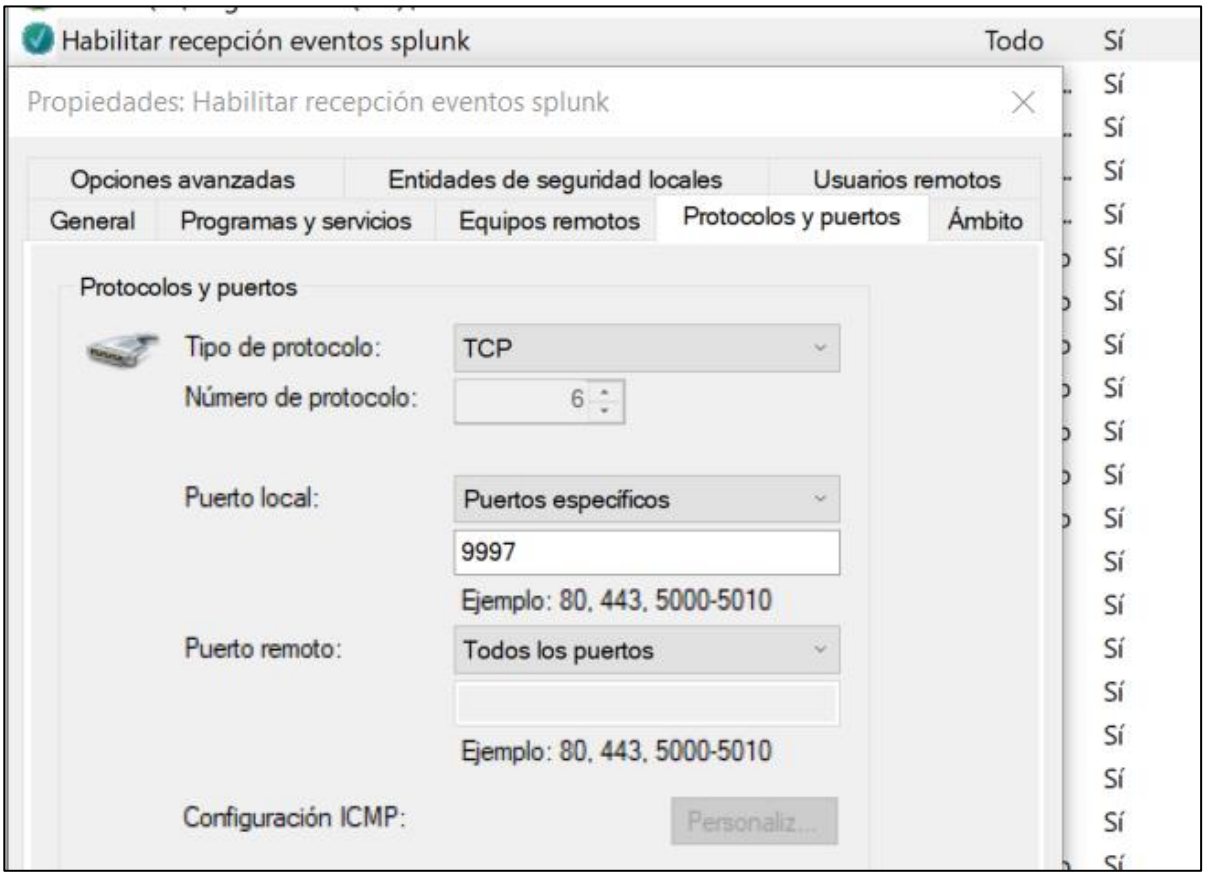


Ilustración 41: Regla en el firewall del equipo de administración para la recepción de eventos en Splunk

Una vez realizado esto habríamos acabado con la configuración inicial del Splunk principal.

3.2 Instalación de Nessus

La instalación de Nessus es muy sencilla. Primero nos iremos a su web oficial donde dispondremos de multitud de opciones para la instalación.

Nessus - 7.2.1

Release Date

10/11/2018

Release Notes:

Nessus 7.2.1

Name	Description	Details
Nessus-7.2.1-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	Checksum
Nessus-7.2.1-Win32.msi	Windows 7, 8, 10 (32-bit)	Checksum
Nessus-7.2.1.dmg	macOS (10.8 - 10.13)	Checksum
Nessus-7.2.1-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	Checksum
Nessus-7.2.1-es5.x86_64.rpm	Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-7.2.1-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-7.2.1-suse11.x86_64.rpm	SUSE 11 Enterprise (64-bit)	Checksum
Nessus-7.2.1-es7.x86_64.rpm	Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-7.2.1-ubuntu1110_i386.deb	Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04 and 17.10 i386(32-bit)	Checksum
Nessus-7.2.1-suse12.x86_64.rpm	SUSE 12 Enterprise (64-bit)	Checksum
nessus-updates-7.2.1.tar.gz	Software updates for Nessus Scanners linked to Nessus Managers in 'offline' mode (all OSes/platforms).	Checksum
Nessus-7.2.1-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	Checksum

Ilustración 42: Opciones para la instalación de Nessus

Una vez descargado, instalaremos el paquete de forma sencilla en la ubicación deseada. Este programa nos ofrece sus servicios a partir de una interfaz web que tendremos disponible en el puerto 8834 por defecto, aunque es un parámetro configurable.

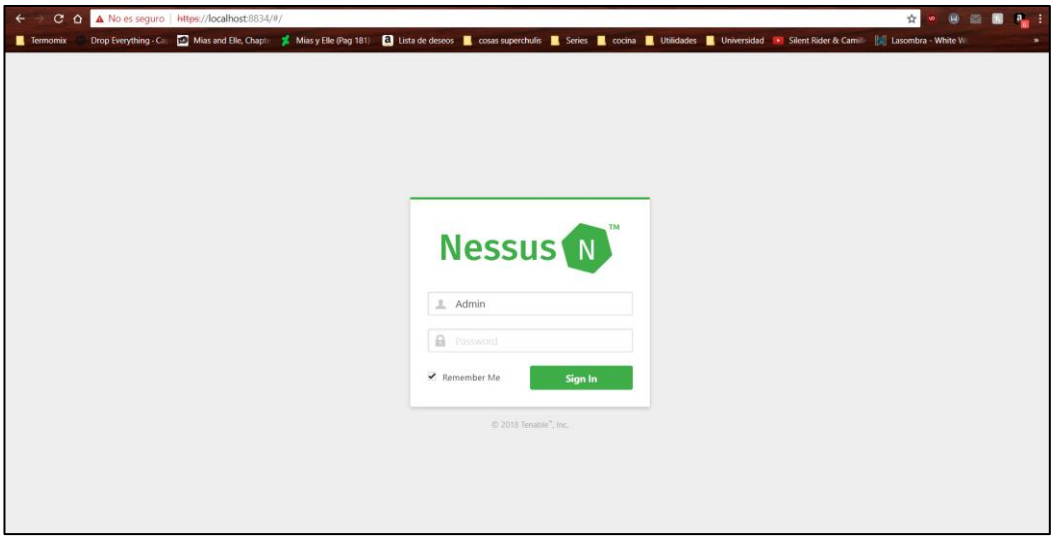


Ilustración 43: Pantalla de Acceso a Nessus

3.3 Realización de los escaneos de la red e integración con Splunk

3.3.1 Opciones generales para los escaneos

Como hemos comentado en los apartados anteriores, Nessus nos proporciona una gran variedad de opciones para realizar los escaneos.

Podremos tener la cantidad de escaneos en progreso que queramos, así como pausarlos y cancelarlos en cualquier momento.

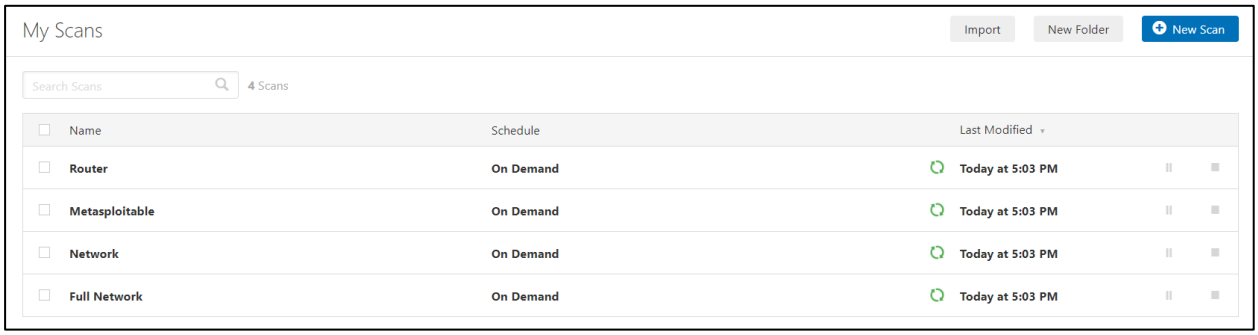


Ilustración 44: Escáneres en ejecución. A la izquierda se pueden ver los botones de pausa y cancelar

Tenemos la posibilidad de programar los escaneos, importar configuraciones y ver cuándo fue la última vez que se realizó un escáner.

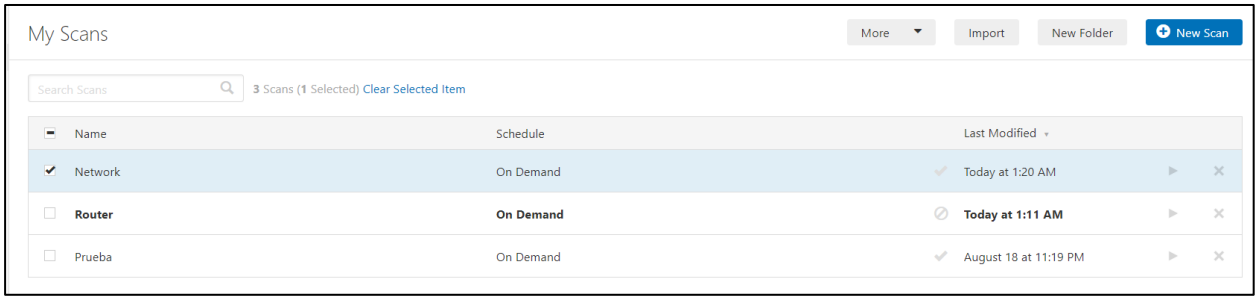


Ilustración 45: Distintas posibilidades sobre los escáneres ya realizados

En el transcurso del análisis podemos ver las vulnerabilidades que se vayan encontrando y su severidad.

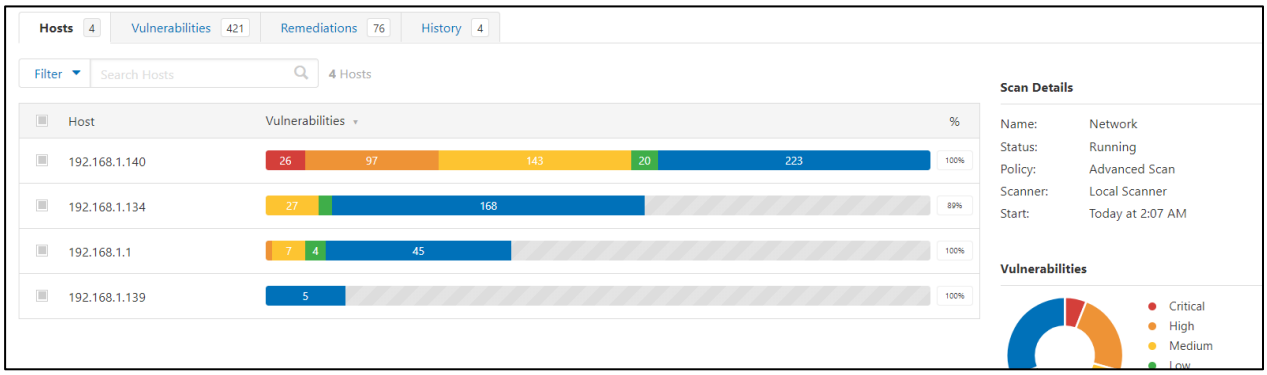


Ilustración 46: Análisis en curso

Cuando creemos un nuevo escáner podremos elegir entre múltiples opciones para escanear: un solo dispositivo, una subred a partir de su IP y asociándole una máscara para ir descubriendo todos los dispositivos o incluso un dominio web.

Nosotros vamos a escanear la red al completo.

3.3.2 Escaneo de nuestra red.

Para escanear la red completa tendremos que poner la IP de la red junto a la máscara de la subred que queramos escanear

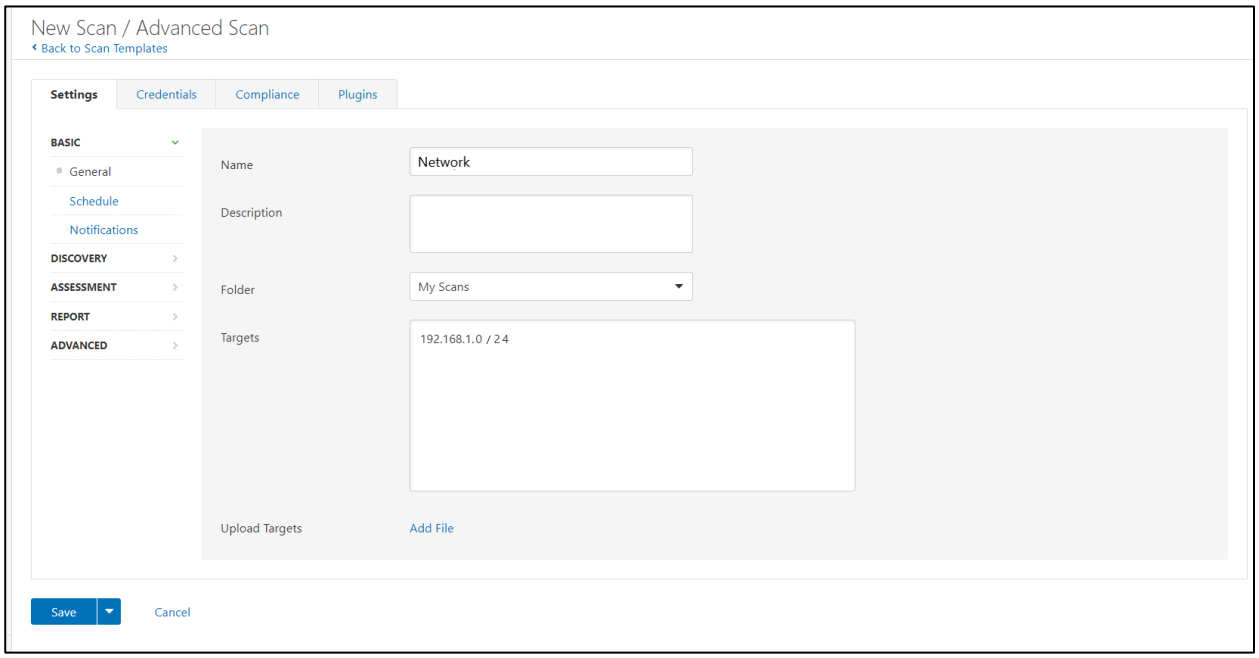


Ilustración 47: Escaneo de la red completa

Usaremos los siguientes plugins:

- **Escaneo de programas maliciosos:** Con Nessus podremos buscar posibles ficheros maliciosos, incluso podemos buscar ficheros específicos por número de hash[2] (md5[3]) ya sea porque sepamos que son maliciosos o para excluirlos como posible resultado.

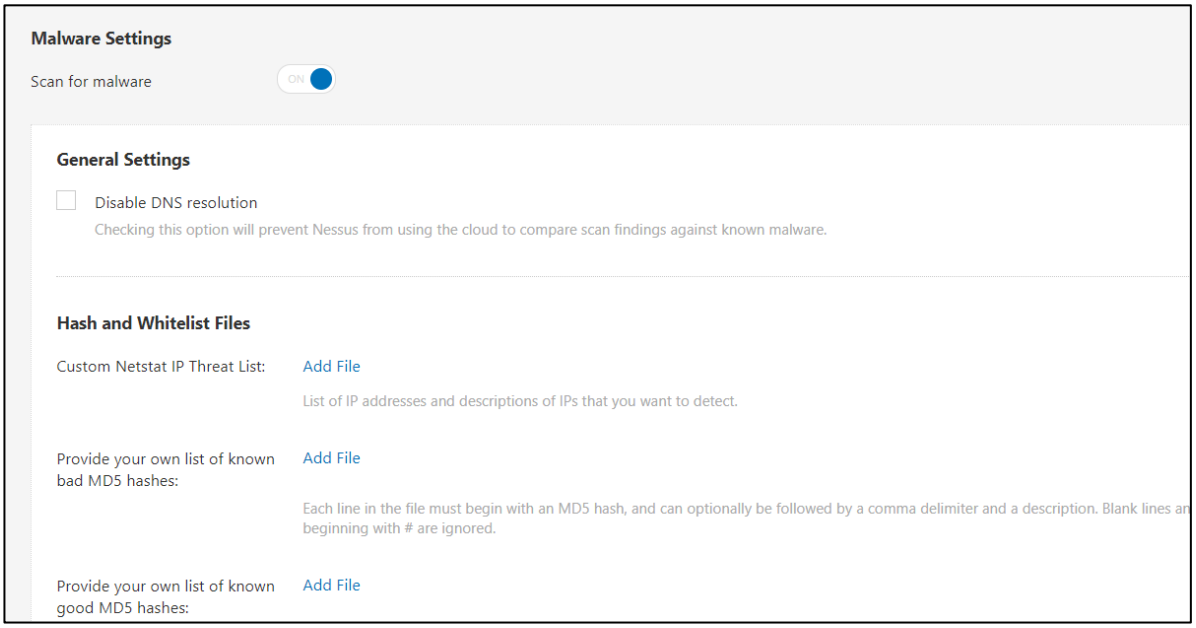


Ilustración 48: Opciones para la búsqueda de ficheros maliciosos.

[2] Se define una función hash como aquella que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte en un rango de salida finito, normalmente cadenas de longitud fija. [59]

[3] MD5 es un algoritmo hash de 128 bits. Algunos de sus usos es el de comprobar que algún archivo no haya sido modificado, que no se haya corrompido al descargarlo o moverlo o comprobar si dos archivos son el mismo. [60]

- **Credenciales:** Este plugin nos permite introducir múltiples métodos de autentificación y credenciales que se usarán en los distintos dispositivos que encontremos en la red.

Definiremos credenciales de acceso para el protocolo ssh, específicamente con las credenciales de los servidores dado que son uno de los dispositivos donde más interés tenemos en encontrar posibles vulnerabilidades.

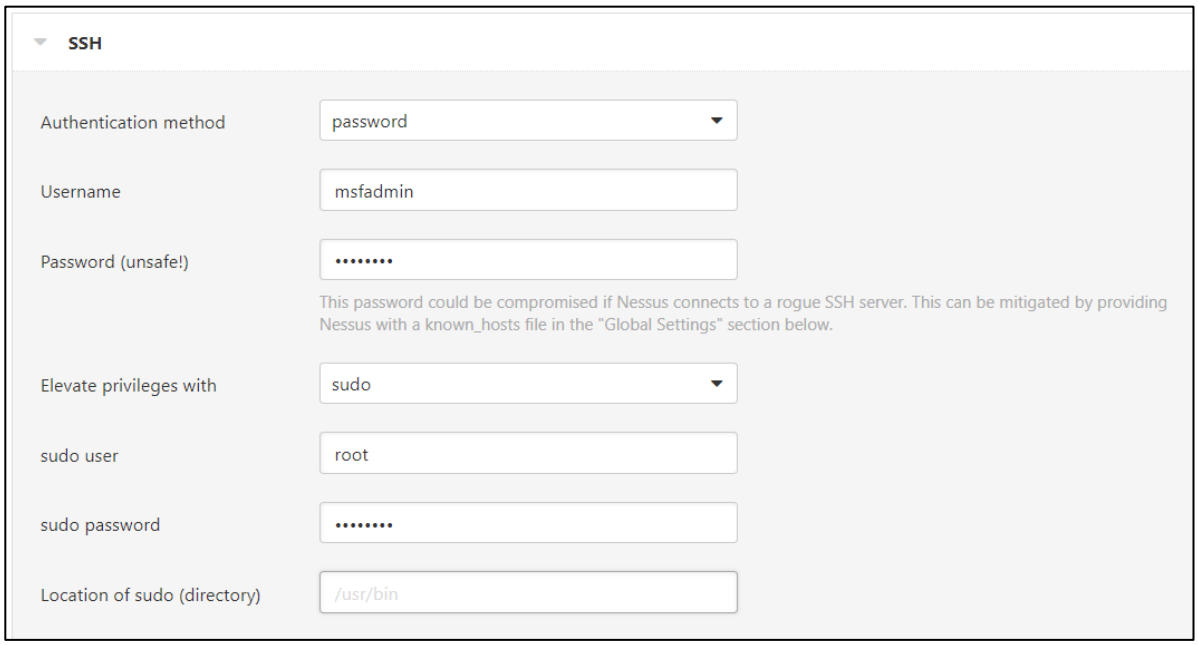


Ilustración 49: Configuración de la autentificación por ssh

También podemos poner credenciales normalmente usadas por defecto (En este caso hemos seleccionado Usuario y contraseña 1234, pero podrían ser otras como admin/admin) para el protocolo http por si alguno de los dispositivos tiene un servicio web y no han cambiado las credenciales por defecto.

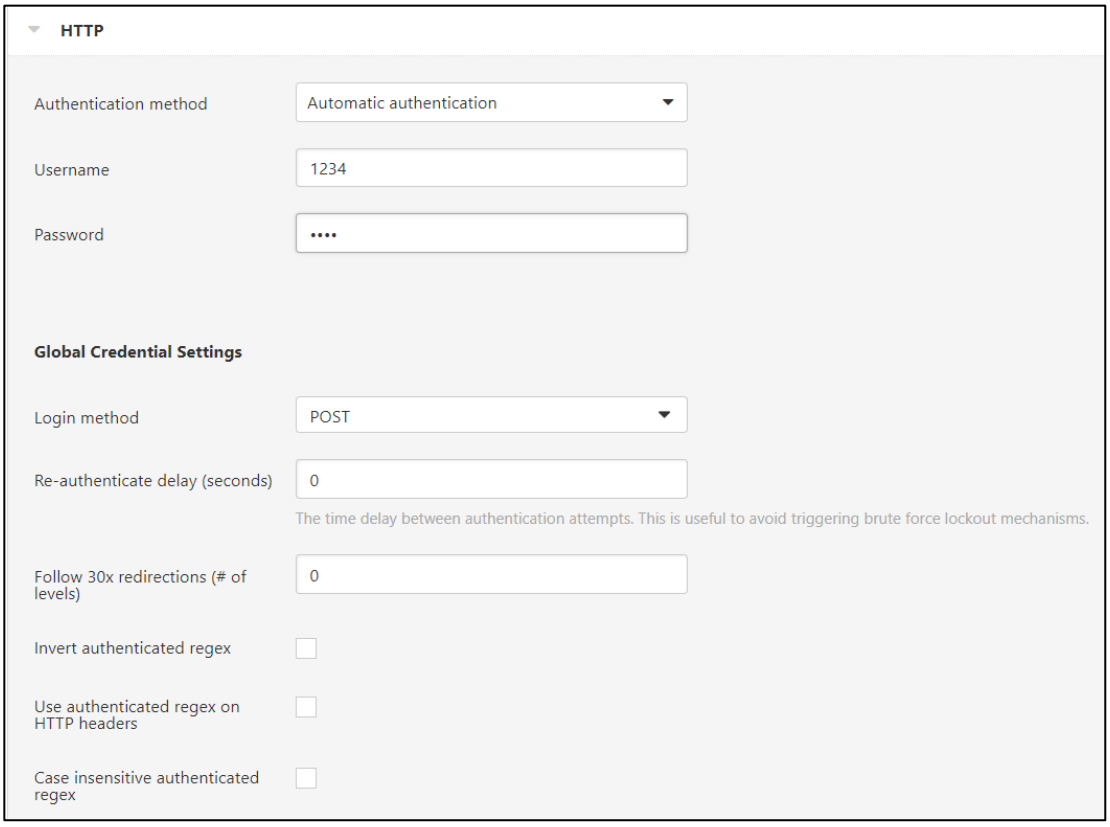


Ilustración 50: Configuración de autentificación por HTTP

Nosotros solo configuraremos esos dos, pero disponemos de multitud de protocolos de autentificación para configurar como FTP, POP2 y POP3 o telnet, protocolos muy habituales, pero también fácilmente explotables.

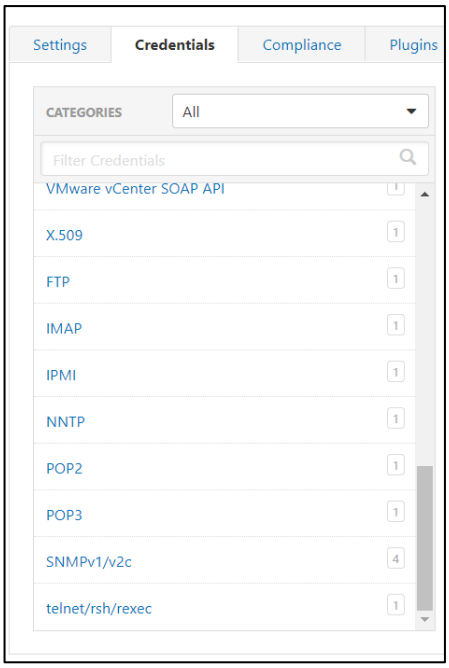


Ilustración 51: Diferentes métodos de autentificación

Hay una gran diferencia entre las vulnerabilidades que se encuentran en dispositivos con sesiones activas y sin ellas. En la ilustración 41 podemos ver la diferencia entre los equipos 192.168.1.134, en el cual teníamos la sesión de Windows activa, y 192.168.1.144 en el cual tenemos Windows en el equipo, pero no una sesión activa, por lo que no se encuentran las mismas vulnerabilidades

Ilustración 52: Dispositivos de la red y sus vulnerabilidades

3.3.3 Integración con Splunk.

Splunk tiene una tienda de aplicaciones que nos facilitan la integración con otras herramientas. En este caso vamos a usar la aplicación que nos permite registrar fácilmente las vulnerabilidades encontradas por los escáneres de Tenable (incluido Nessus) en Splunk, por lo que procedemos a su instalación desde la tienda.

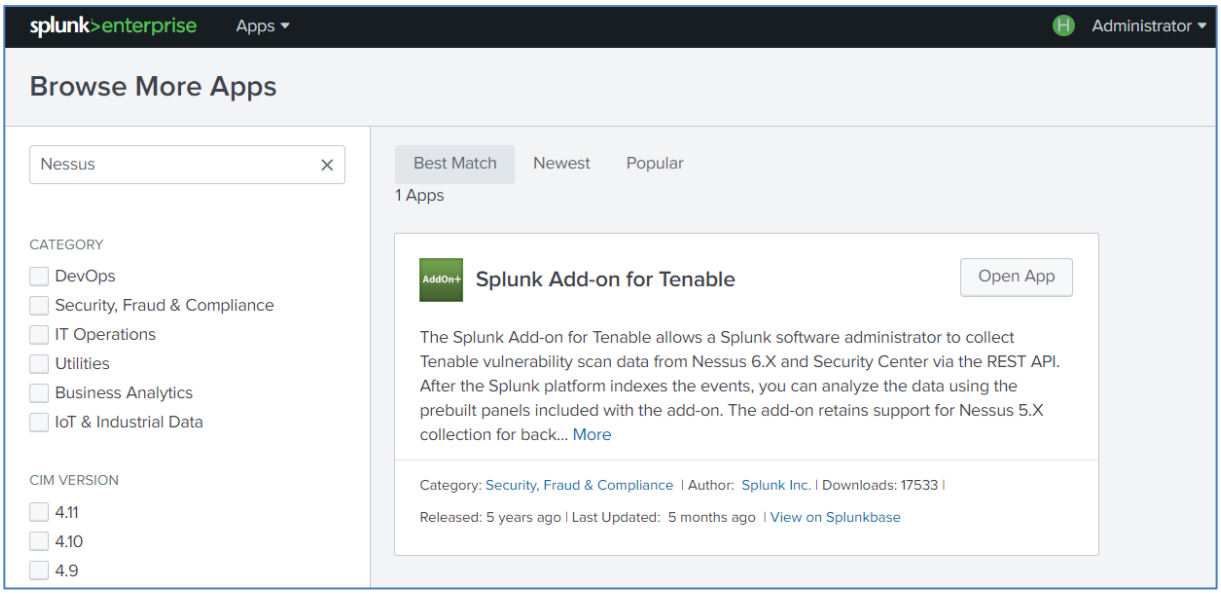


Ilustración 53: Aplicación para la integración de Nessus con Splunk

Como podemos ver, una vez que instalamos la aplicación en Splunk necesitaremos configurarla. Para ello debemos poner los datos de la instancia de Nessus que queremos asociar.

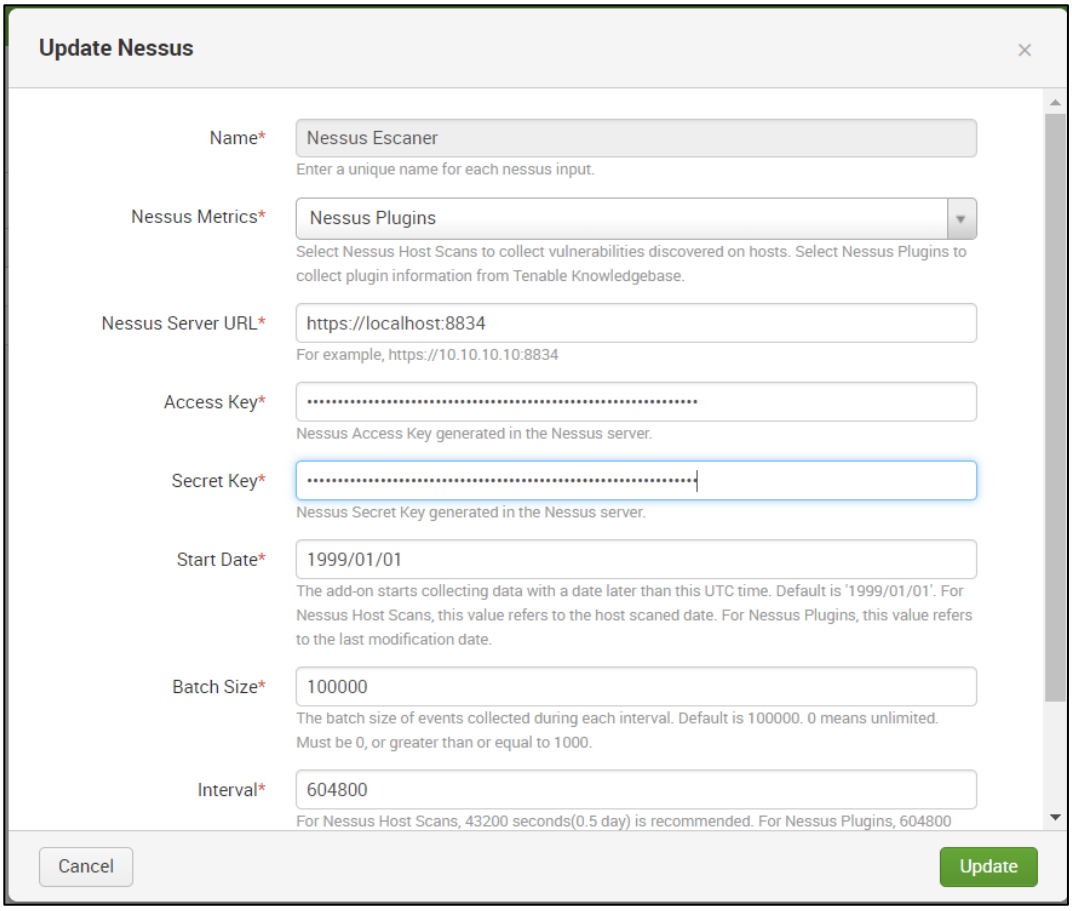


Ilustración 54: Configuración del escáner en Splunk

Los datos que necesitamos los podemos encontrar en la configuración de Nessus.

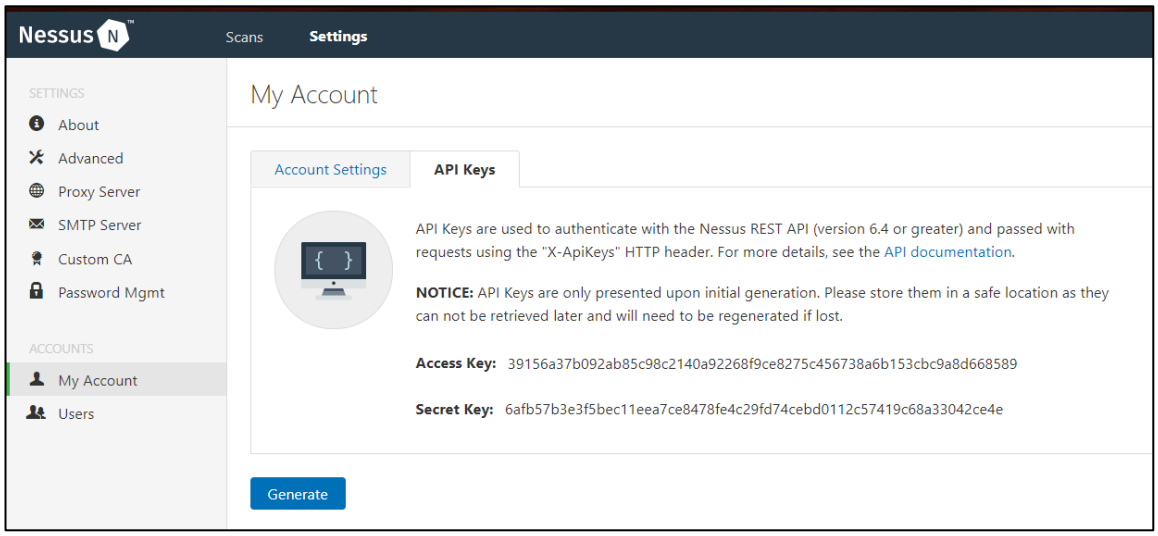


Ilustración 55: Localización de los identificadores únicos de Nessus

Podemos crear alertas, como vemos en la cabecera de la imagen, para que cuando salgan nuevas vulnerabilidades de alerta crítica recibamos una notificación, podemos ver el histórico de vulnerabilidades encontradas en los escaneos y los porcentajes de vulnerabilidades por severidad.

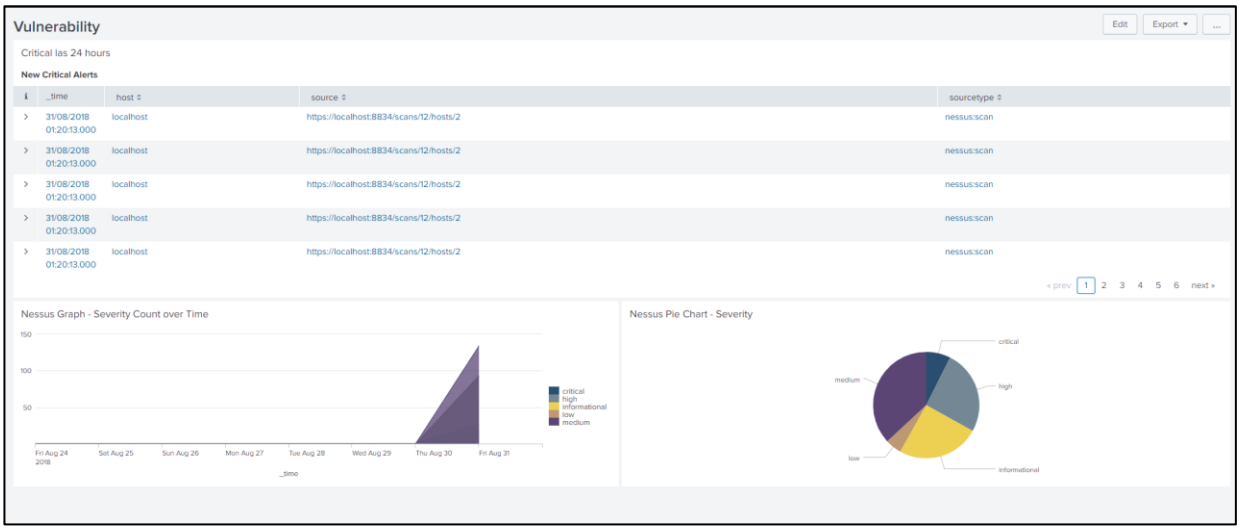


Ilustración 56: Dashboards para la vista de las vulnerabilidades en Splunk

Cuando recibamos los datos de los nuevos escaneos, aquellas vulnerabilidades que ya existían no serán reportadas nuevamente y por tanto no harán saltar las alertas en Splunk ni recibiremos notificaciones repetidas.

3.3.4 Errores con los certificados de Nessus:

Uno de los problemas que encontramos en la integración de Nessus con Splunk fue un problema con los certificados ya que Nessus usa el protocolo https, pero no disponíamos de certificados SSL [41] registrados en la máquina donde tenemos desplegados Nessus y Splunk. Esto es necesario dado que estamos trabajando en una red interna, por ello debemos tener los certificados en local.

Este error fué finalmente fácil de localizar dado el propio índice que tiene Splunk para sus logs de ejecución y errores. Al no poder visualizar los eventos relacionados con las vulnerabilidades encontradas en Nessus, simplemente tuvimos que buscar en este índice y pudimos ver que teníamos un problema con los certificados.

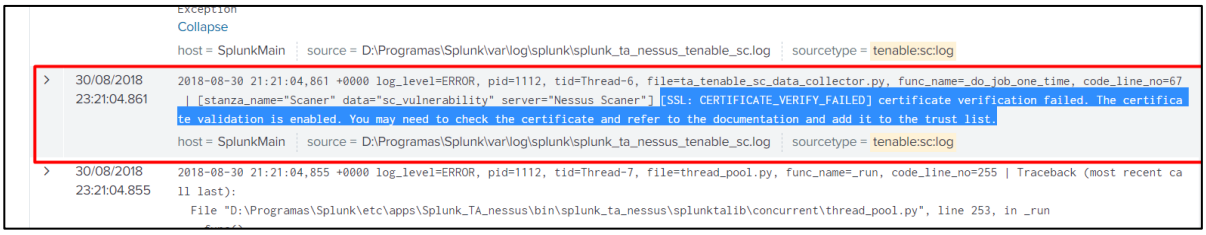


Ilustración 57: Certificado Invalido

Para conseguir ver los eventos en Splunk tuvimos que exportar el número de serie de los certificados SSL de Nessus en el equipo donde estamos trabajando para poder configurarlos como de confianza [42].

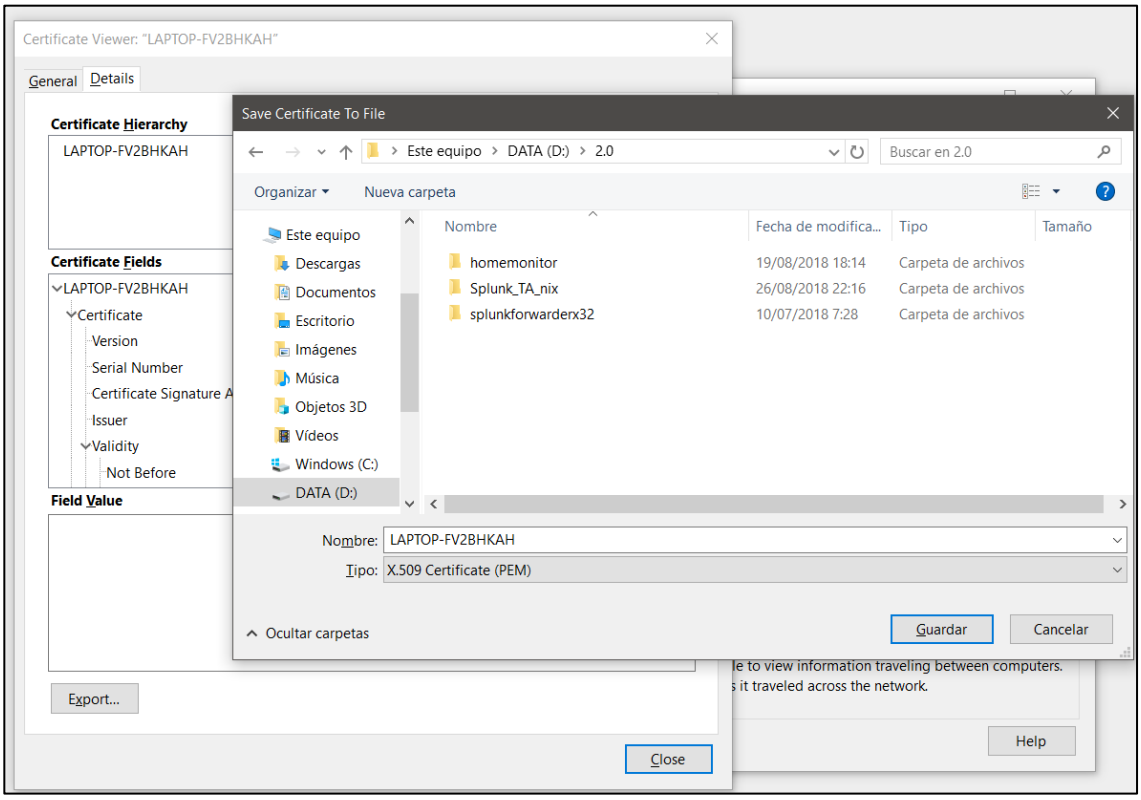


Ilustración 58: Exportación de los certificados

Una vez exportados, los tendremos que añadir al fichero cacerts.txt de la aplicación que nos permite la integración de Nessus con Splunk, en concreto en la carpeta: *Splunk\etc\apps\Splunk_TA_nessus\bin\splunktalib\httplib2*

```
-----END CERTIFICATE-----

# Certificate for Nessus App

-----BEGIN CERTIFICATE-----
MIIDvTCCAqWgAwIBAgIDAO8NMA0GCSqGSIb3DQEBCwUAMIGdMRwwGgYDVQQKDBNO
ZXNzdXMgVXNlcnMgVW5pdGVkMScwJQYDVQQLDB5OZXNzdXMgQ2VydGlmaWNhdGlv
biBBdXRob3JpdHkxETAPBgNVBAcMCE5ldyBZb3JrMQswCQYDVQQGEwJVUzELMAkG
A1UECAwCTlkxJzAlBgNVBAMMHk5lc3N1cyBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0
eTAeFw0xODA4MTIxOTAwNTdaFw0yMjA4MTExOTAwNTdaMH0xHDAaBgNVBAoME05l
c3N1cyBVc2VycyBVbml0ZWQxFjAUBgNVBAsMDU5lc3N1cyBTZXJ2ZXIxETAPBgNV
BAcMCE5ldyBZb3JrMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTlkxGDAWBgNVBAMM
D0xBUFRPUC1GVjJCSEtBSDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AN9uHmb6FoGj8tsawBz3YtKpGeAeT0oz3H1XjQrbg2dLM/8c8PomYcHRIK4X4JF5
v8CyQ9+RHcU9uCPb4hQu0FKPd3N8wINbHu5700pyC6/xosh5tedLy/mgiD3Bw7cE
hdLeZn/4Aafl9fxy20Q75V2onBifURvSa/BvtEMrEtVN2e8luXwvfTwRREYYD3Vr
VB0ibpUDZ139CQ3NNUoUb1NOa5/sNSfjPH4IVcLKxo2Akwb4YA6ZiBCnApFHsqEY
N7Prr0Zg3vlgxmhkFuEIZ3tZhWKcKJwn13R8ztRrBBo39FoK6+KSpTebO4dZspzi
UrklriNEv4V0eJBZbCK8jtUCAwEAAaMlMCMwEQYJYIZIAYb4QgEBBAQDAgZAMA4G
A1UdDwEB/wQEAwIF4DANBgkqhkiG9w0BAQsFAAOCAQEANus1bcLM7WbLZyqfmNce
j+fEwrRu/NJsWWJqbocALGjHyfErPm4gRDZoXkh0ZV5ABEfVNHuyv8hjDNXuwY72
bMjBH/vSJBgdVWT+E1N7cFUAAMIRTeiejfSSlkb8y8bW1S7LVb5BLc7CV1T+LsuW
ELFJ48iqsKWLzxmSTHz8v3UbkdOTwHp5lt8UP7zrTB6SLk3qEzSlEdsdL3nkz++e
HwjHUiqa/yATmYjSePVlP2fnlDUlO3jNstM3Wg72msuUKBNUu74NVtf+vxQc+St+
mwc22Or6yCWB6e8uHmAm7VYj9qE23d4icfGR9KIGcIykIY8fZvNYuTX6V2aiXXiK
lw==
-----END CERTIFICATE-----
```

Ilustración 59: Inserción de los certificados para Splunk

Y podremos encontrar finalmente los eventos relacionados con las vulnerabilidades encontradas por Nessus en el índice que hemos creado específicamente para ello.

Cada vez que se encuentra una vulnerabilidad no registrada previamente, podremos ver un nuevo evento en el índice que nos dará la información sobre ésta.

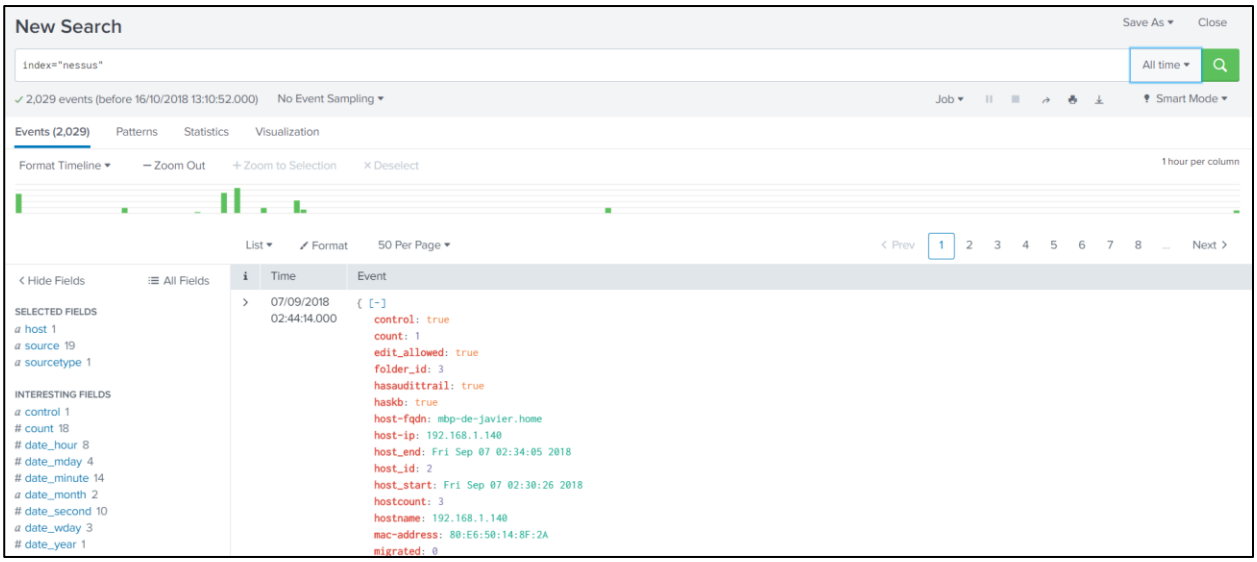


Ilustración 60: Resultados de los escaneos

3.4 Análisis de los resultados

Nessus nos categoriza las alertas según la prioridad de la vulnerabilidad, que se refiere a su posible afección a la seguridad de los sistemas.

Una vez tengamos los resultados Nessus, podemos ver con facilidad todas las vulnerabilidades encontradas y así determinar cuáles son las que afectan más a la operativa de la empresa.

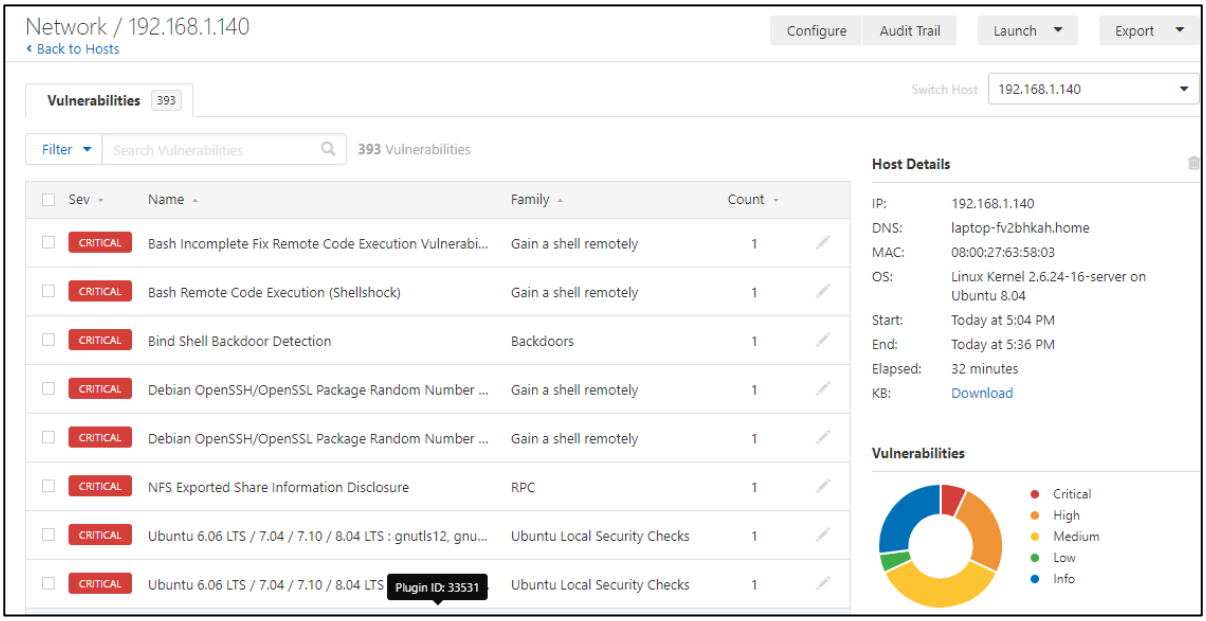


Ilustración 61: Lista de vulnerabilidades encontradas en un dispositivo

Nessus no solo nos ofrece la posibilidad de ver las vulnerabilidades encontradas, también podemos ver lo que podemos hacer para remediarlas.

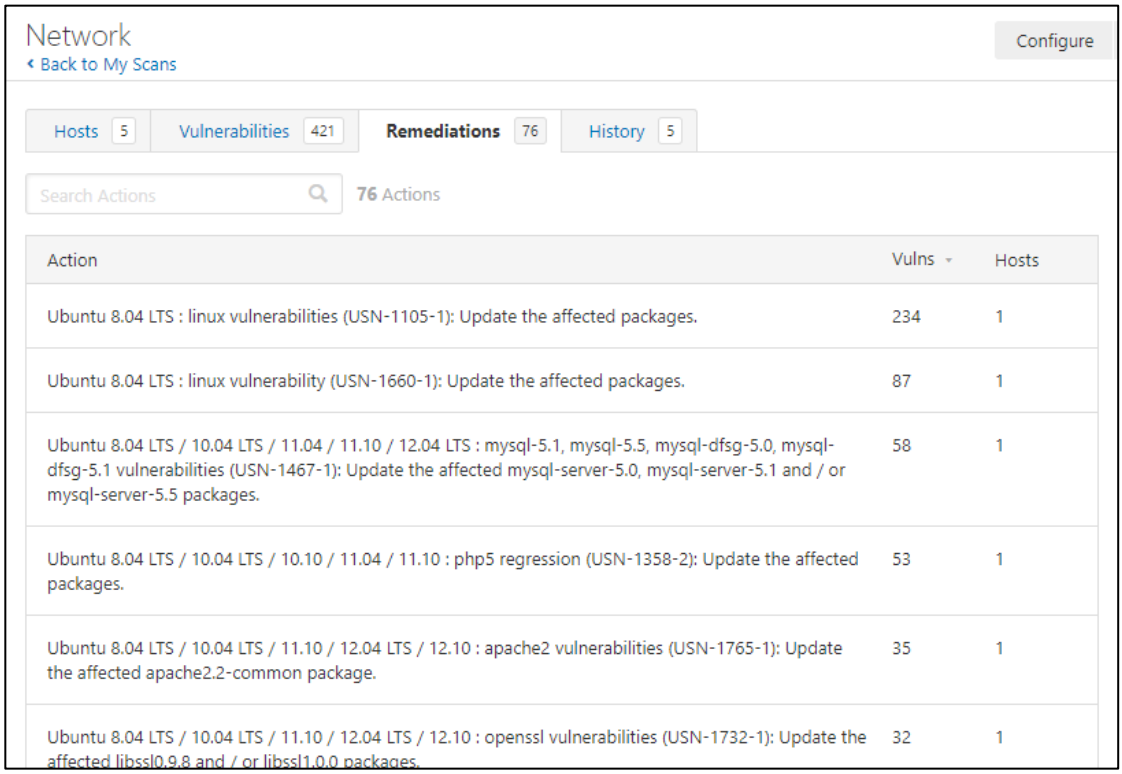


Ilustración 62: Correcciones para las vulnerabilidades

En este caso hemos procedido a actualizar múltiples paquetes de Ubuntu:

```
The following packages will be upgraded:
  apache2 apache2-mpm-prefork apache2-utils apache2.2-common apparmor
  apparmor-utils apt apt-utils base-files bash bsdutils bzip2 console-setup
  cron dash dhcp3-client dhcp3-common dpkg dpkg-dev eject fastjar file
  friendly-recovery fuse-utils gzip initramfs-tools initscripts
  installation-report iproute klibc-utils libapr1 libaprutil1 libbz2-1.0 libc6
  libc6-dev libc6-i686 libcupsys2 libcurl3-gnutls libdbus-1-3 libexpat1
  libfreetype6 libfuse2 libgnutls13 libhtml-parser-perl libklibc libldap-2.4-2
  libldap2-dev liblwres30 libmagic1 libmysqlclient15off libnewt0.52
  libntfs-3g23 libpam-modules libpam-runtime libpam0g libpam0g-dev
  libpango1.0-0 libpango1.0-common libparted1.7-1 libpcre3 libpng12-0 libpq5
  libsasl2-2 libsasl2-modules libtasn1-3 libtiff4 libtomcat5.5-java
  libvolume-id0 libwww-perl libxml2 linux-libc-dev login logrotate lsb-base
  lsb-release lshw lvm2 module-init-tools mount mysql-client-5.0 mysql-common
  mysql-server mysql-server-5.0 nfs-common nfs-kernel-server ntpdate openssl
  parted passwd pciutils php5-cgi php5-cli php5-common php5-gd php5-mysql
  postfix postgresql-8.3 postgresql-client-8.3 postgresql-client-common
  postgresql-common procps python-apt python-central rsync samba samba-common
  sudo sysv-rc sysvutils tasksel tasksel-data tomcat5.5 tomcat5.5-admin
  tomcat5.5-webapps tzdata udev ufw update-manager-core util-linux
  util-linux-locales vim-common vim-tiny w3m wget whiptail xkb-data
126 upgraded, 0 newly installed, 0 to remove and 13 not upgraded.
Need to get 88.2MB/96.0MB of archives.
After this operation, 9372kB of additional disk space will be used.
Do you want to continue [Y/n]?
```

Ilustración 63: Actualizaciones de Ubuntu

Después de realizar las actualizaciones, volveremos a realizar los escaneos.

Gracias al histórico de Nessus podemos ver cuándo se han realizado los distintos escaneos y qué diferencias se han encontrado entre ellos con su herramienta *Diff*.

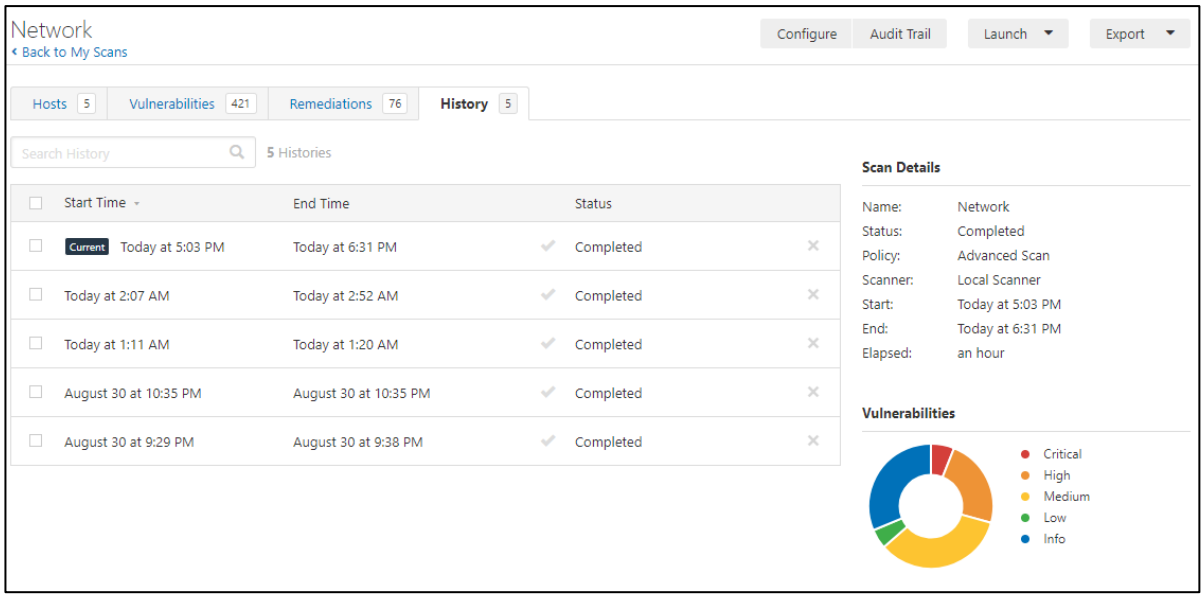


Ilustración 64: Histórico de Nessus

Seleccionamos los escaneos que queremos comparar y cuál será el de referencia.

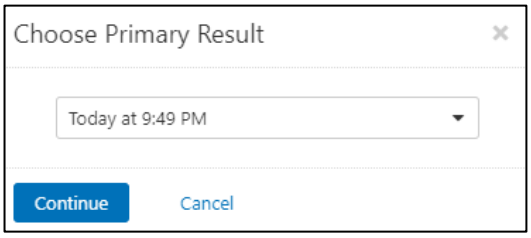


Ilustración 65: Seleccionamos el escáner que queremos que sea de referencia

Podemos ver gracias a esto la importancia de mantener actualizados los sistemas con los que trabajamos, ya que después de una primera ronda de actualizaciones hemos corregido 11 vulnerabilidades críticas, así como 60 altas y 108 medias.

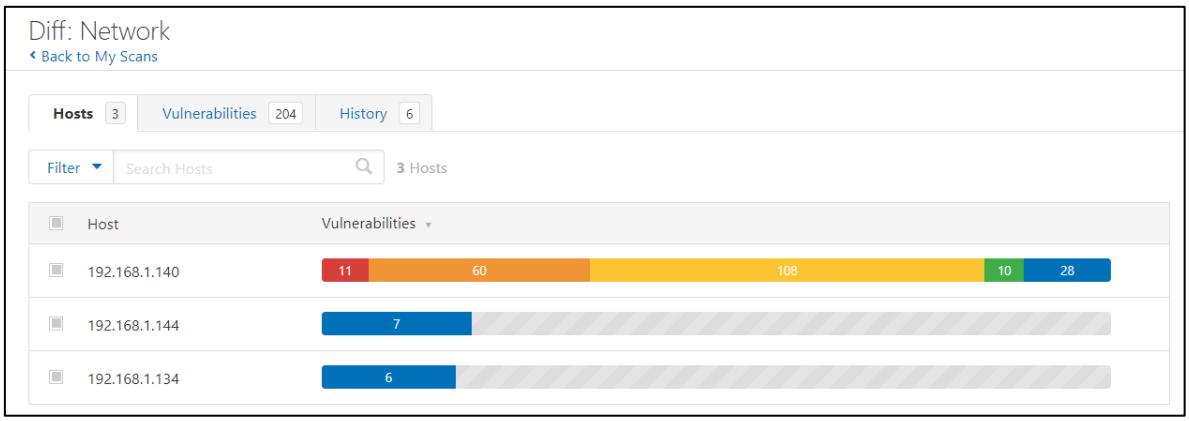


Ilustración 66: Diferencia entre los escaneos después de las actualizaciones

3.4.1 Caso de Uso: Detección de un ataque por desplazamiento lateral

Una de las alertas más críticas que tenemos es que Nessus ha detectado que tenemos varios puertos abiertos que no requieren autentificación para entrar en el sistema:

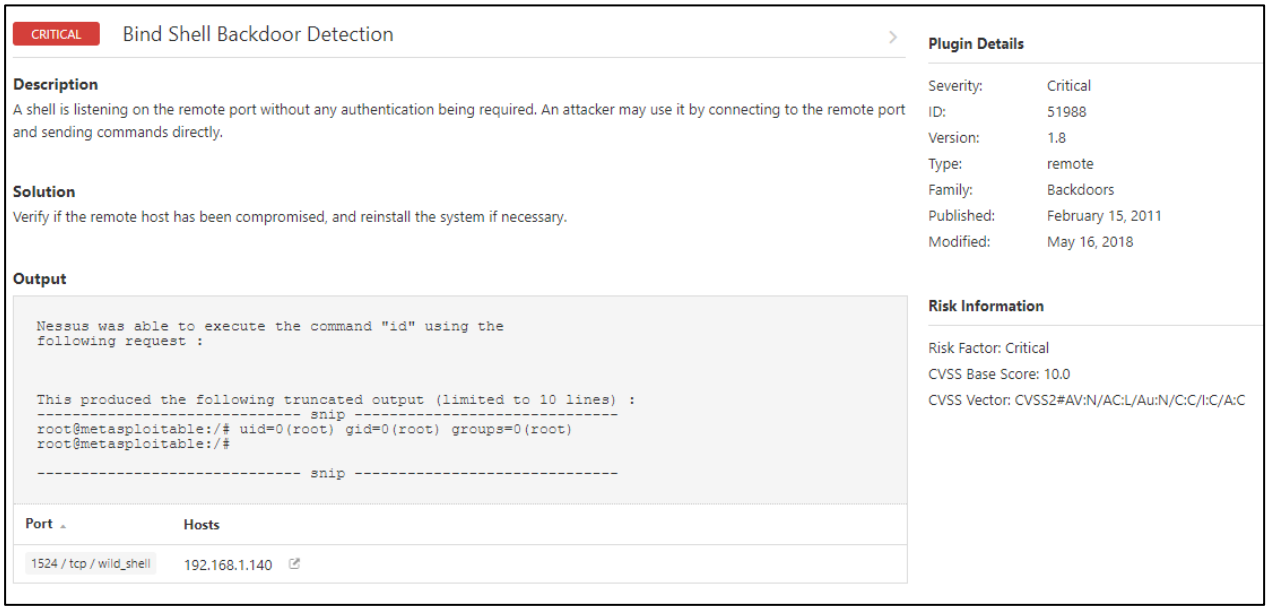


Ilustración 67: Alerta crítica, no se requiere autentificación

Nos basaremos en esta vulnerabilidad para la configuración de las alertas de Splunk.

En este caso, como comentamos en el punto 1.3.5: “Intentaremos detectar un ataque mediante la técnica de desplazamiento lateral, en el cual un atacante se aprovecha de este tipo de vulnerabilidades de autentificación para expandirse a través de la red. Estaremos buscando intento de autentificación hacia los equipos vulnerables, ya que una vez que el atacante se encuentre dentro de cualquiera de nuestros dispositivos, intentará tomar el control de otros. Nos centraremos en las conexiones que usen el protocolo SSH dado que es el que más comúnmente se usa y es el que nos da más control sobre la máquina hacia la que dirigimos el ataque.”

Los accesos a los sistemas de los equipos Ubuntu (en los cuales hemos detectado esta vulnerabilidad) se registran en el fichero de log ***var/log/auth.log*** [43] , por lo que monitorizaremos este archivo para detectar intentos de autentificación y crear alertas cuando detectemos una nueva entrada en este fichero.

3.5 Despliegue de los forwarders de Splunk

Hasta ahora habíamos desplegado el Splunk principal, que es el que usaremos como índice global para todos los eventos de la red, y Nessus, que nos ha permitido realizar los escáneres de la red, y hemos integrado la información de este último en Splunk para tener alertas en el caso que se detecten nuevas

A continuación, acabaremos con el despliegue de Splunk instalando los forwarders en los distintos equipos que queremos monitorizar. Los forwarders se encargarán de enviar los datos que queramos monitorizar al Splunk principal que hemos desplegado previamente. Serán ejecutados como servicios en segundo plano, al igual que se ejecuta el splunk principal.

Primero realizaremos un despliegue inicial de un forwarder universal y otro completo para comprobar la configuración y ver que todo es correcto. Una vez realizado el despliegue inicial se podría usar el Deployment server para instalar los forwarders en el resto de los dispositivos de la red.

3.5.1 Forwarder universal:

Dado que este forwarder no tiene interfaz web podremos realizar su configuración de dos formas:

Por línea de comandos, los cuales modificarán los ficheros de configuración del forwarder:

```
msfadmin@metasploitable:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server SplunkMain:8999
Your session is invalid.  Please login.
Splunk username: admin
Password:
Added forwarding to: SplunkMain:8999.
msfadmin@metasploitable:/opt/splunkforwarder/bin$
```

Ilustración 68: Añadir un forwarder por CGI

O enviando los ficheros ya creados con la configuración deseada por sftp:

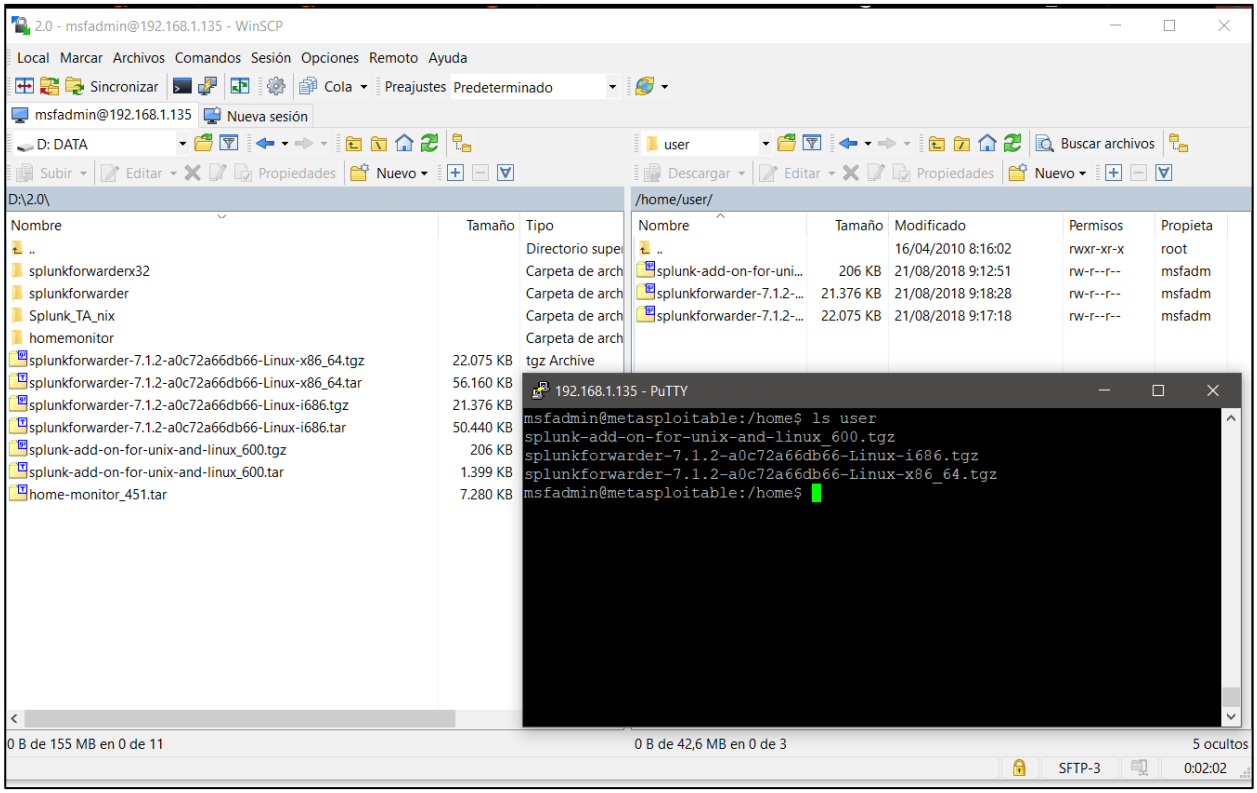


Ilustración 69: Envió de ficheros por sftp

Los ficheros de configuración los guardaremos en la carpeta **local** dentro del directorio donde hayamos instalado Splunk. Haremos esto para que en el caso de actualizar los programas de Splunk (ya sea el propio forwarder o las aplicaciones que podamos estar usando para realizar la integración con otras herramientas) se mantenga la configuración y no tengamos que volver a realizarla.

Para definir hacia dónde vamos a mandar la información en este tipo de forwarders tendremos que configurar el fichero ***outputs.conf*** o realizarlo por línea de comandos como vemos en la figura 62.

En nuestro caso, al enviarse simplemente del forwarder al indexador principal la información, y estar estos en la misma subred, solo tendremos que definir el nombre de este y el puerto hacia el que mandaremos la información.

```
3  # This file contains outputs.conf.  The use this file is to configure
4  # forwarding in a distributed set up.
5  #
6  # To use one or more of these configurations, copy the configuration block into
7  # outputs.conf in $SPLUNK_HOME/etc/system/local/. You must restart Splunk to
8  # enable configurations.
9  #
10 # To learn more about configuration files (including precedence) please see the
11 # documentation located at
12 # http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
13
14
15 # You can specify a target group for an IP:PORT which consists of a single receiver.
16 # This is the simplest possible configuration; it sends data to the host at
17 # SplunkMain on port 9997.
18
19 [tcpout]
20 defaultGroup = laboratorio
21
22 [tcpout:laboratorio]
23 server = SplunkMain:9997
```

Ilustración 70: Fichero outputs.conf

Dada la cantidad de variables a monitorizar en Ubuntu, usaremos el fichero de configuración ***inputs.conf*** para definir los ficheros de logs y los puertos que queremos monitorizar.

new 1 | inputs.conf

```
116
117 [script://./bin/hardware.sh]
118 sourcetype = hardware
119 source = hardware
120 interval = 36000
121 disabled = 1
122
123 [monitor:///Library/Logs]
124 disabled = 1
125
126 [monitor:///var/log]
127 whitelist=(\.log|log$|messages|secure|auth|mesg$|cron$|acpid$|\.out)
128 blacklist=(lastlog|anaconda\.syslog)
129 disabled = 0
130
131 [monitor:///var/adm]
132 whitelist=(\.log|log$|messages)
133 disabled = 0
134
135 [monitor:///etc]
136 whitelist=(\.conf|\.cfg|config$|\.ini|\.init|\.cf|\.cnf|shrc$|^ifcfg|\.profile|\.rc|\.rules|\.tab|tab$|\.l
137 disabled = 0
138
139 ### bash history
140 [monitor:///root/.bash_history]
141 disabled = false
142 sourcetype = bash_history
143
144 [monitor:///home/*/.bash_history]
145 disabled = true
146 sourcetype = bash_history
147
```

Ilustración 71: Variables a monitorizar

3.5.2 Forwarder Completo

Configuraremos un forwarder completo mediante la instalación de un paquete Splunk Enterprise. Es el mismo paquete, pero debemos cambiar la configuración para que envíe los eventos hacia el indexador principal.

Encontraremos la opción en el menú de la esquina superior derecha en **Settings → Forwarding and receiving → Forward data → Add new**. En esta ventana podremos introducir la IP del indexador principal, así como el puerto al que queremos que se envíen los eventos.

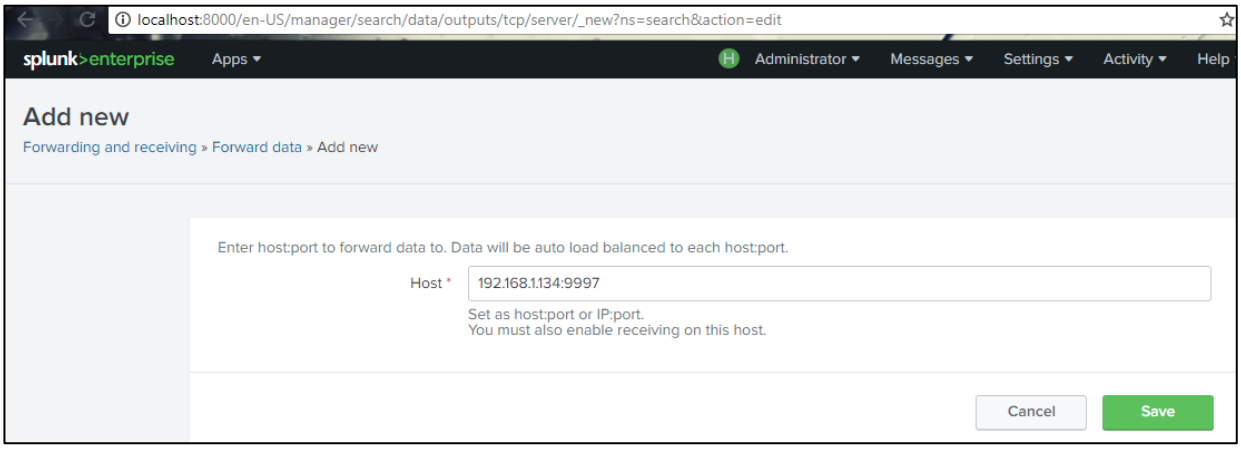


Ilustración 72: Configuración del forwarder para que envié la información al indexador principal

Una vez configurado el envío de los datos, seleccionaremos qué datos queremos enviar desde el menú principal.

Desde este tipo de forwarder es mucho más sencillo añadir la información que queremos monitorizar ya que Splunk nos ofrece directamente una lista de eventos que queremos recoger. Podemos configurar también el cómo los recoge y cada cuánto tiempo, así como en que índice queremos guardarlos. El nombre de este índice tiene que seguir ciertos patrones y además existir en el splunk principal porque si no, este no será capaz de indexar los eventos

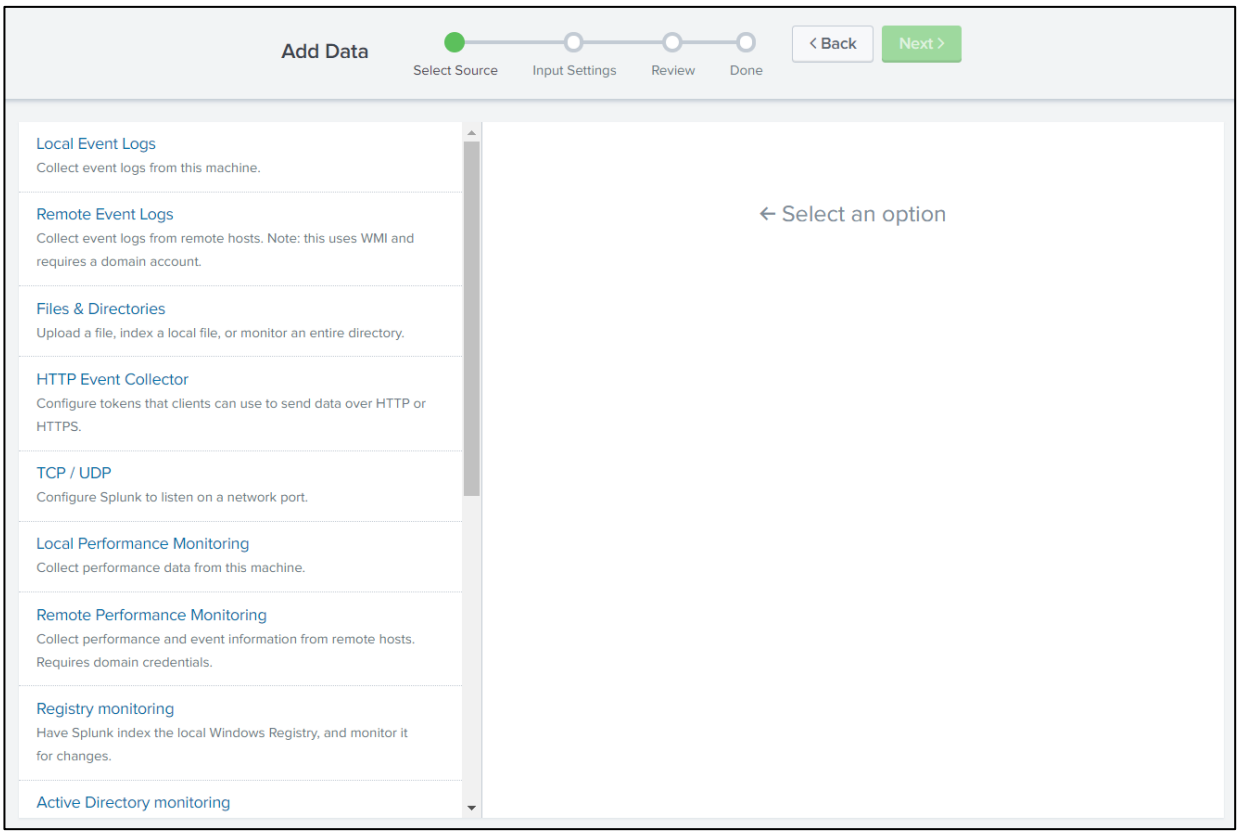


Ilustración 73: Menú principal para añadir eventos a monitorizar en Splunk

Para nuestro caso de uso nos interesan principalmente los ficheros de registro de autenticaciones, por lo que serán los que nos centraremos en configurar.

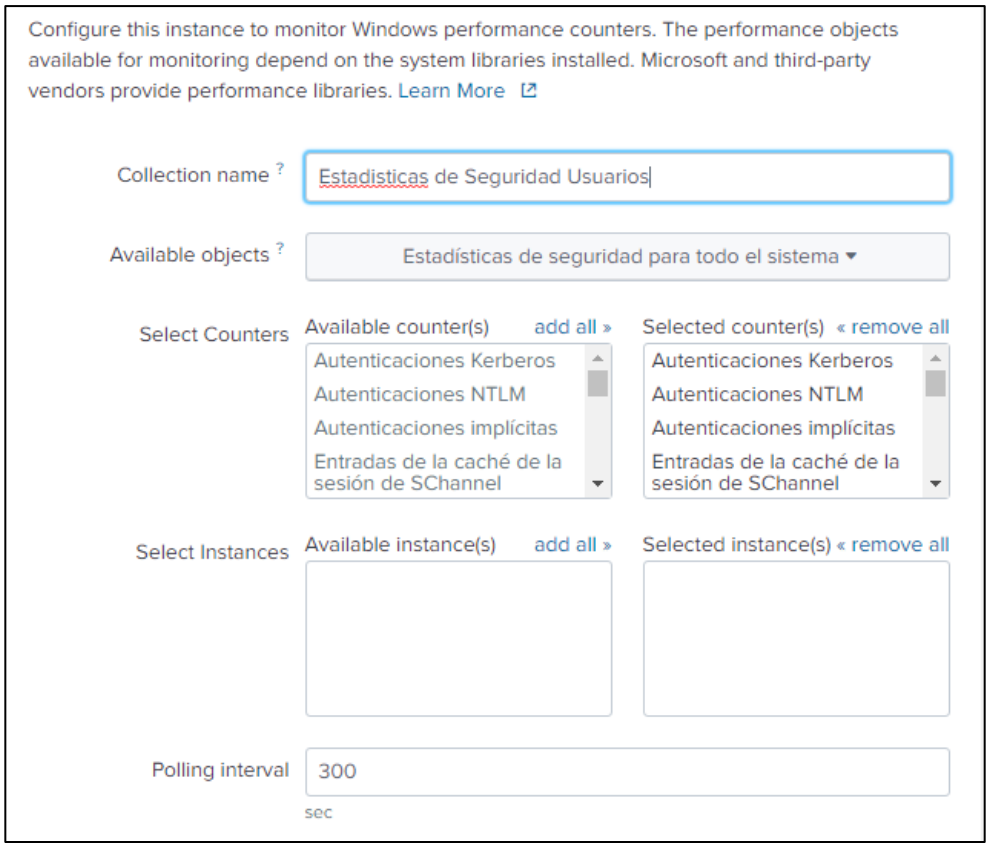


Ilustración 74: Logs de Autenticaciones

Como podemos ver en la imagen, la configuración para Windows con el forwarder completo es mucho más sencilla dado que nos permite visualizar todas las variables que tenemos disponibles y seleccionar las que queramos, no tenemos que ir buscando cuales son los registros de Ubuntu y creando una entrada por cada uno en el fichero de configuración.

Desde Splunk podremos configurar que se registren todo tipo de datos, por ejemplo, el estado de un equipo.

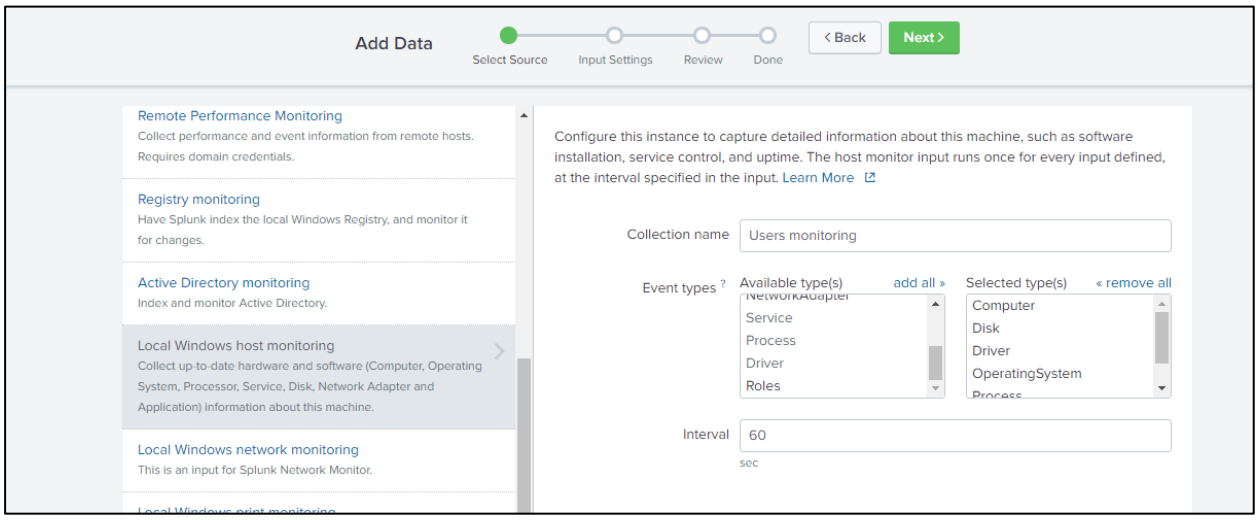


Ilustración 75: Monitorización del estado de la maquina

No necesitamos que sea un tráfico específico ni un formato de log, Splunk está capacitado para darles el formato adecuado a los logs gracias a la gran cantidad de tipos de datos que acepta y a la posibilidad de programar nuestros propios tipos de datos y cómo queremos que se recopilen gracias a la API de Splunk. [44]

Una vez acabados de configurar los forwarders, Splunk nos permite ver el tráfico de datos que estos generan.

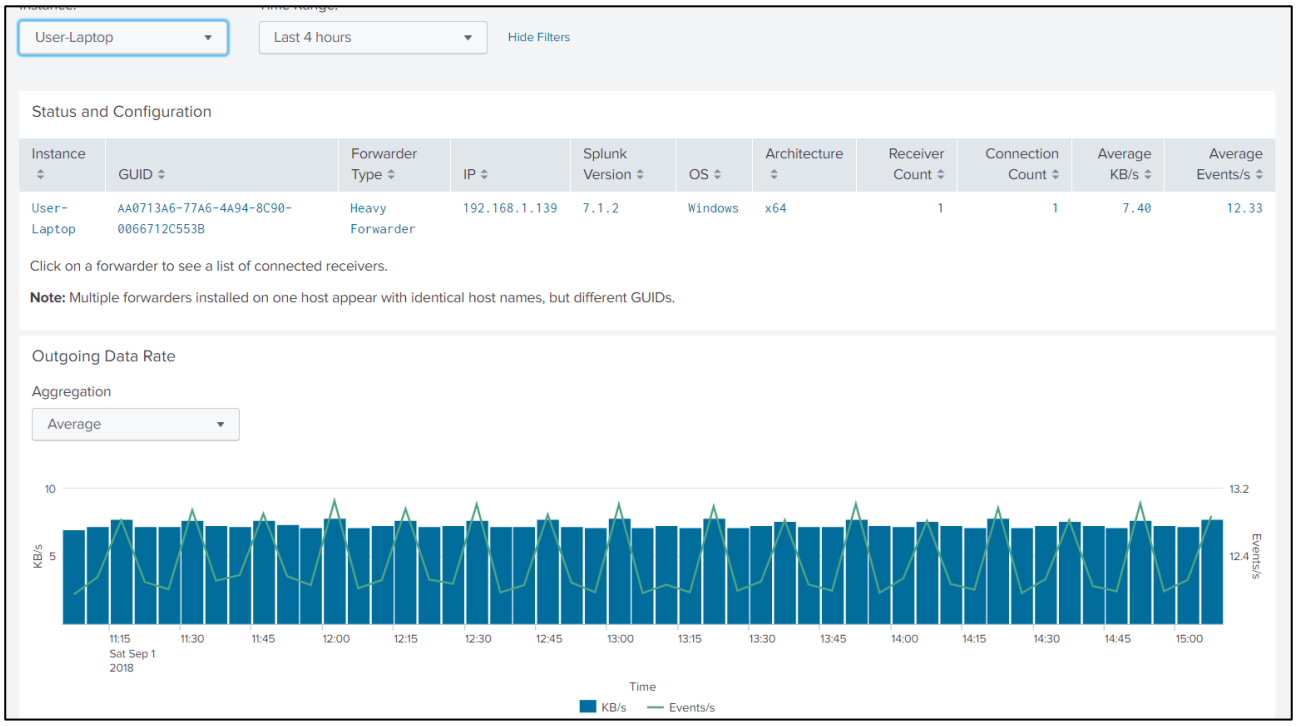


Ilustración 76:Tráfico de datos entre el forwarder y el indexador principal

Y también los logs de una máquina específica gracias a los distintos índices que podemos crear.

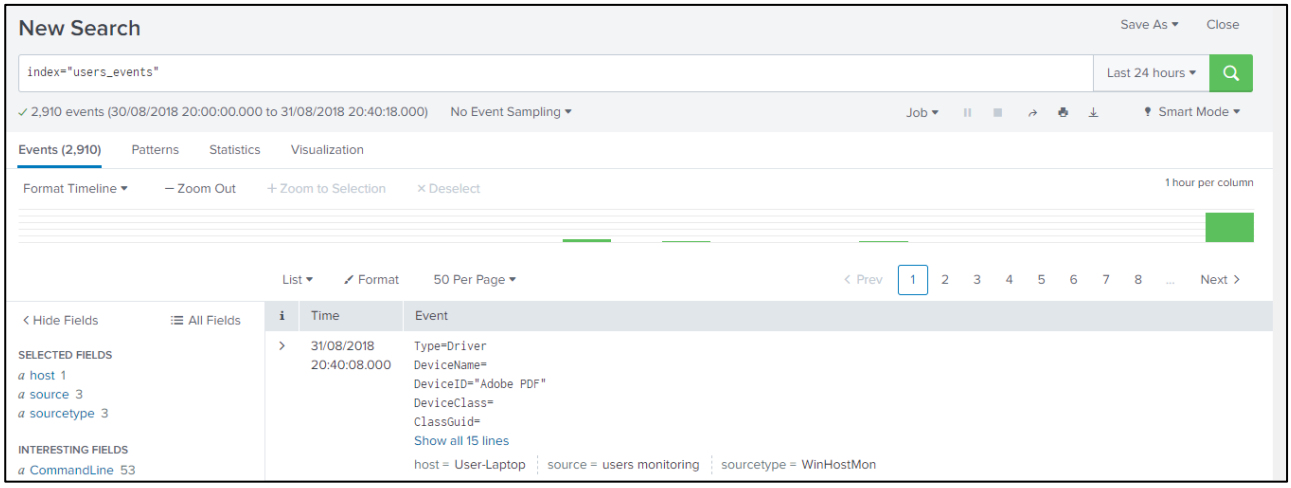


Ilustración 77: Registros de los eventos de usuario

Como hemos creado un índice solo para los eventos de usuario (como vemos en la figura de arriba), tendremos facilidad para encontrar los logs asociados a éstos en esta lista, así no mezclaremos esta información con la que recibimos desde otro tipo de equipos.

3.6 Creación de casos de uso y alertas

Primero determinaremos qué pueden usar los atacantes para explotar las vulnerabilidades encontradas. En este caso al ser varios los puertos que tenemos abiertos, vamos a monitorizar el fichero de logs del sistema, el cual registra los intentos de autentificación en la máquina que estamos monitorizando. Cada vez que se cree una nueva entrada en el fichero, se producirá un evento que se registrará en Splunk.

La manera más fácil de crear las alertas es realizar una búsqueda a través de Splunk buscando los eventos que queramos monitorizar. En este caso nosotros estaremos buscando intentos de autentificación, los cuales se registran en el fichero de *var/log/auth.log* de los servidores de la empresa.

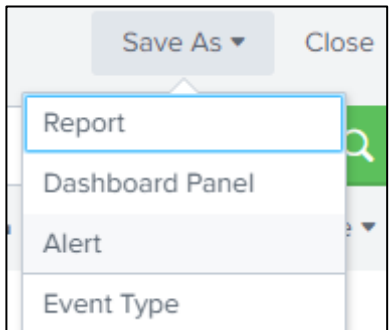


Ilustración 78: Creación de alertas a partir de búsquedas

A partir de estas búsquedas, una vez la tengamos afinada y veamos los eventos que buscamos, podemos crear una alerta. Esta alerta saltará cada vez que se produzca un nuevo evento que coincida con la búsqueda.

Tenemos múltiples opciones de configuración de las alertas:

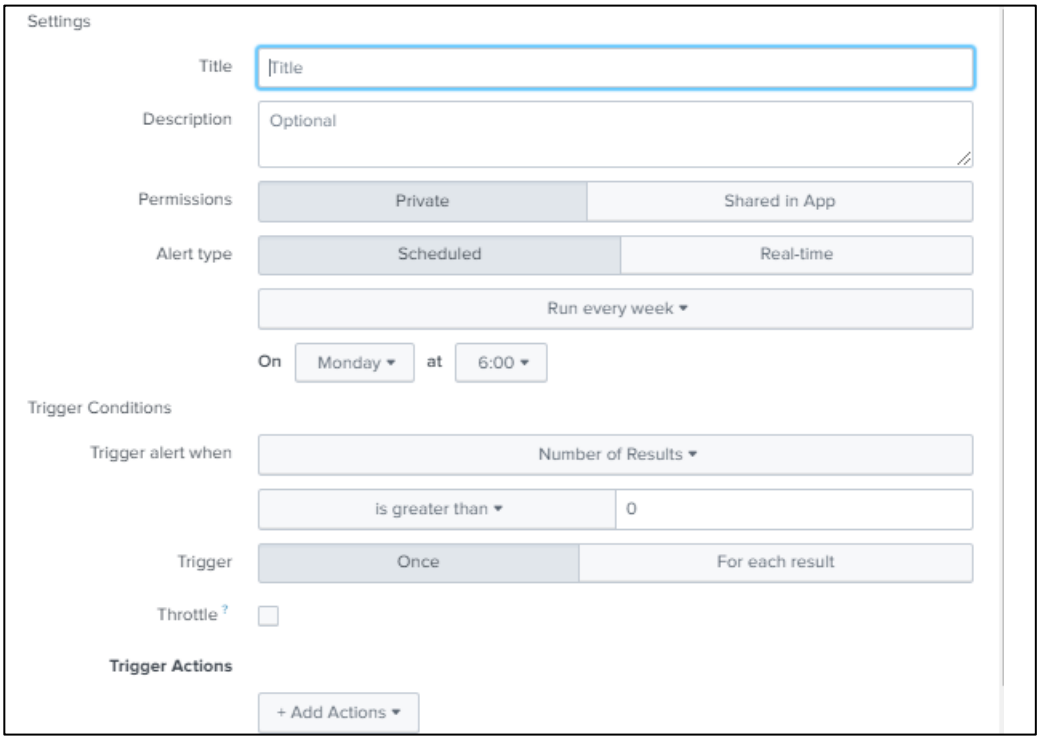


Ilustración 79: Configuración de una alerta

Las opciones de configuración irán cambiando según lo que seleccionemos y tendremos que configurar unos parámetros u otros.

Lo primero que debemos configurar será el nombre de la alerta. También podemos añadir una descripción, aunque esta no es obligatoria.

Lo siguiente serán los permisos: **Private** solo muestra la alerta a la persona que la ha creado y **Shared in App** se la muestra a todos los usuarios configurados en el despliegue de Splunk.

Después vendrá lo más importante: En qué tiempo y en qué condiciones saltará la alerta. Aquí es donde más cambiarán los datos a configurar, ya que no es lo mismo una alerta programada que una en tiempo real. Además podemos definir distintos valores para los cuales salte la alerta (Trigger alert when…)

Las búsquedas de las alertas pueden estar programadas para realizarse cada cierto tiempo y que salte la alerta si se cumplen ciertas condiciones o puede ejecutarse constantemente y saltar en otros casos. Las condiciones de la alerta pueden ser el número de resultados, de host, de fuentes o personalizado (según otros campos del log) y podremos programar que nos notifique solo una vez o cada vez que se supere el umbral marcado.

La parte más complicada de la configuración es sin duda la gestión del tiempo dado que si no determinamos correctamente el intervalo de tiempo que queremos analizar, podremos tener alertas repetidas o incluso alertas que no corresponden con lo que estamos buscando.

Las alertas en tiempo real no tienen por qué dar resultados, dado que por la precisión que presenta Splunk, los eventos deben producirse exactamente al mismo tiempo que el escaneo, lo cual no siempre ocurre, por lo que lo mejor es programar búsquedas cada cierto tiempo. A la hora de programar estas búsquedas, si queremos que se realicen de manera consecutiva en el tiempo para que se estén monitorizando siempre los resultados, tenemos que tener en cuenta que no deben solaparse los intervalos de tiempo, dado que si no tendremos alertas repetidas.

Para definir correctamente estos intervalos y que no se solapen usaremos *expresiones de tiempo de Cron* [45], las cuales se usan para la planificación de tareas programadas [46] .

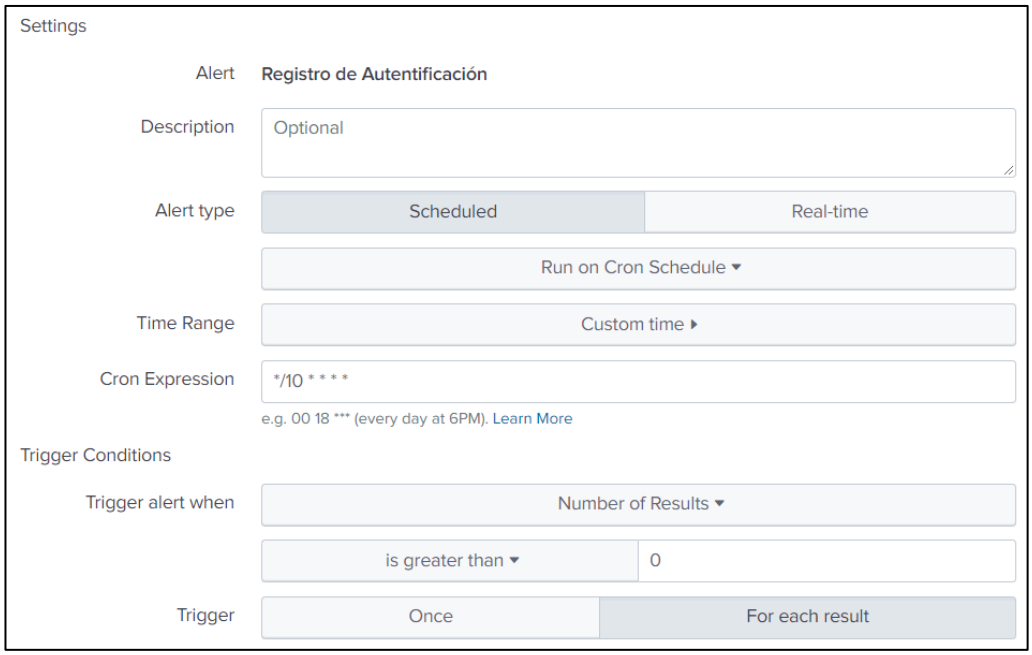


Ilustración 80: Configuración de alertas para el registro de autenticación

En nuestro caso hemos definido que la búsqueda se realice cada 10 minutos (*/10 * * * *) y que salte ante cualquier evento (*greater than 0*), ya que queremos tener una alerta nueva cada vez que se cree una nueva línea en el registro.

Si seleccionamos la opción **Throttle** podremos evitar que, una vez se ha generado una alerta, esta vuelva a saltar, evitando así posibles alertas repetidas, en determinadas circunstancias:

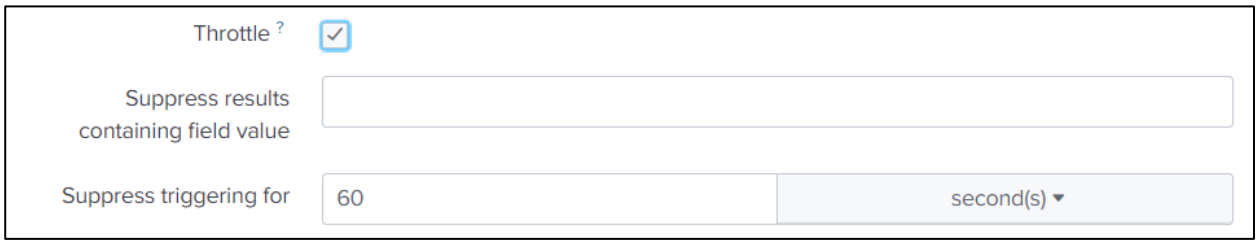


Ilustración 81: Opciones de Throttle

Podremos suprimir alertas con ciertos valores o por un intervalo de tiempo una vez después de la primera.

Finalmente configuraremos qué acción (o acciones) queremos que se ejecute una vez salta una alerta. Splunk dispone de múltiples opciones para gestionar las alertas:

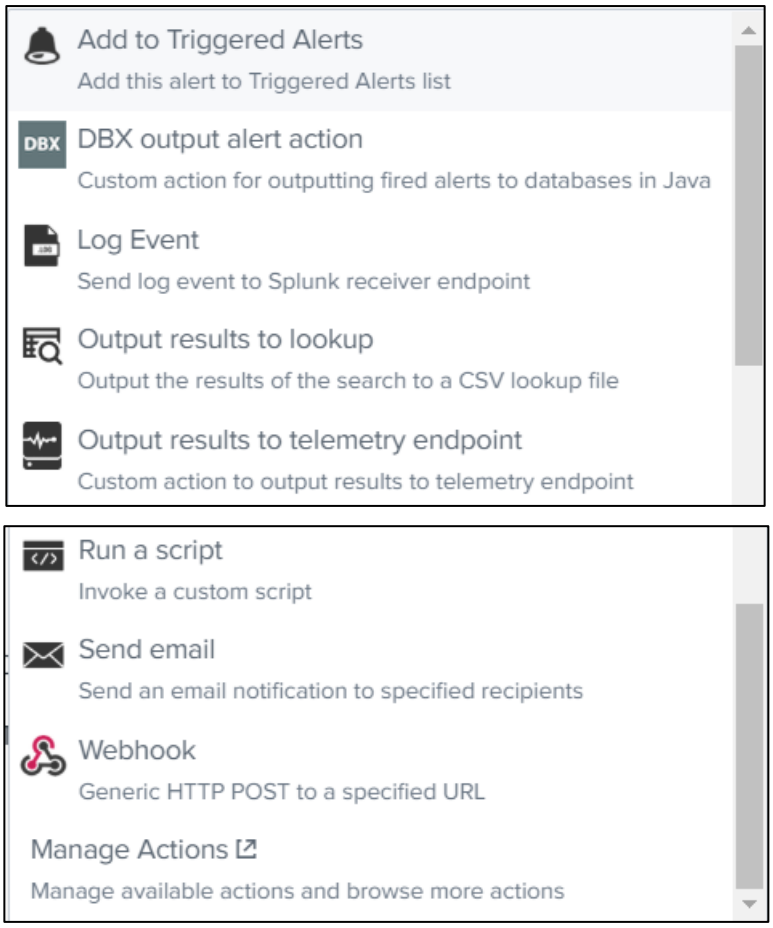


Ilustración 82: Diferentes operaciones a realizar en caso de que salte una alerta

Nosotros nos centraremos en la opción de enviar un email, dado que es lo que hemos decidido que pase para que nos avise de las nuevas alertas encontradas. Este email se enviará desde la cuenta de correo que hemos configurado en el apartado 3.1 cuando hemos configurado el indexador principal, pero el email al que queremos que se envíen las alertas lo podemos configurar para cada una, en caso de que distintas alertas sean gestionadas por personas diferentes.

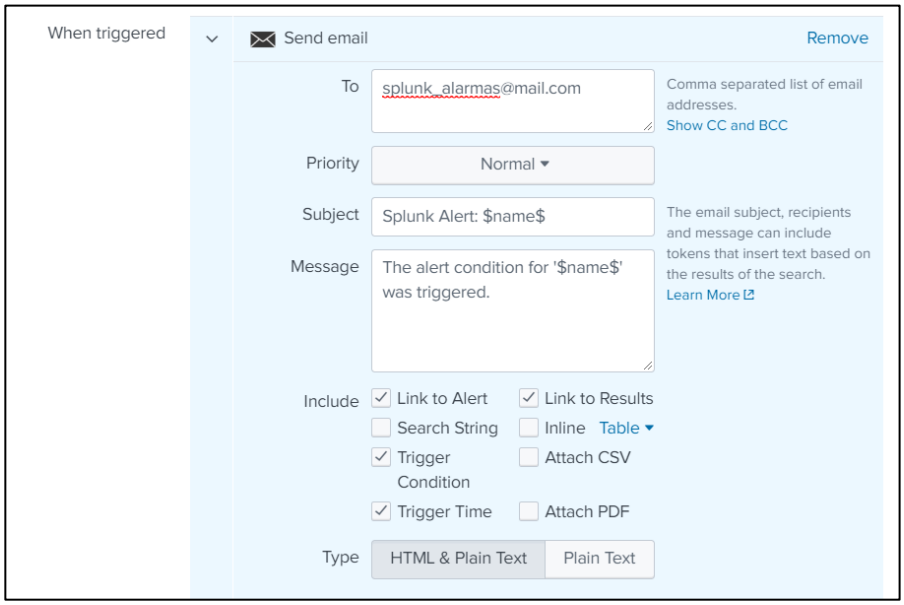


Ilustración 83: Configuración de la alerta enviada por correo

3.7 Visualización de las alertas y de las estadísticas de la red

Hemos elegido recibir alertas por email en caso de que se detecte una nueva autenticación. En el apartado 3.1 hemos asociado a Splunk una cuenta de Gmail que será la que envíe los emails con la información de las alertas. Podemos ver estos emails en la bandeja de enviados de esta cuenta.

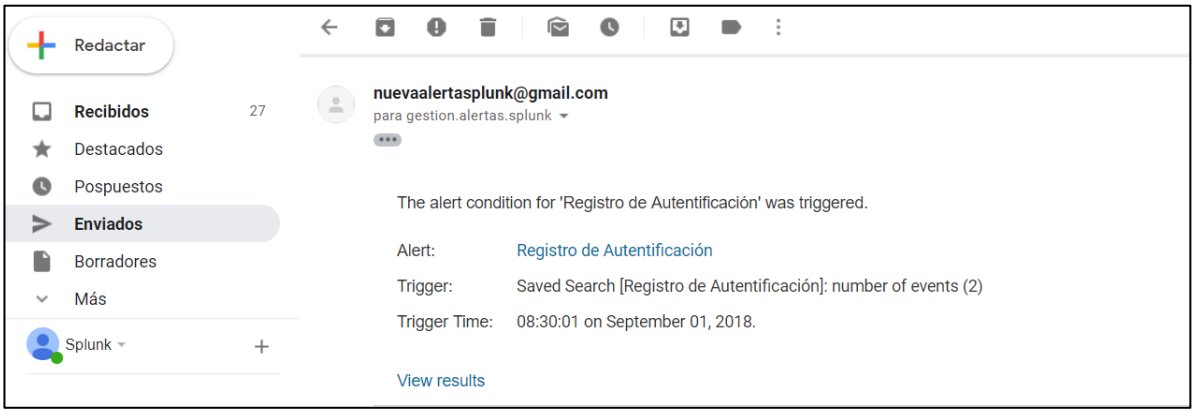


Ilustración 84: Bandeja de enviados del correo configurado en Splunk para notificar las alertas

Y los emails recibidos en la bandeja de entrada de la cuenta que hemos configurado en el apartado 3.6 una vez que se registra un nuevo evento en la búsqueda que hemos configurado.

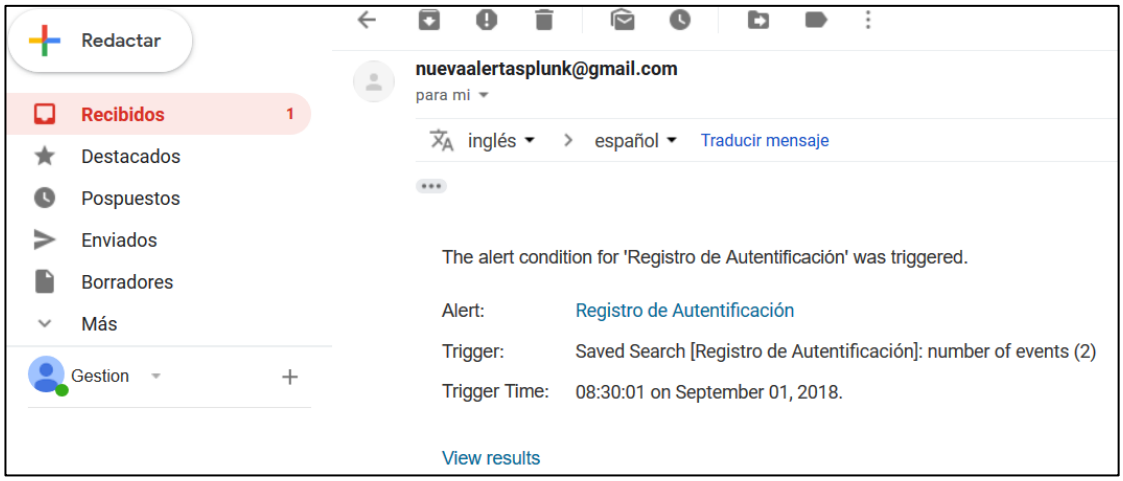


Ilustración 85: Alertas recibidas

Según lo que configuremos en las opciones de Email de la alerta nos llegará una información u otra en el email. En este caso, hemos incluido el enlace de *View Results* que nos llevará a la búsqueda que ha generado la alerta.

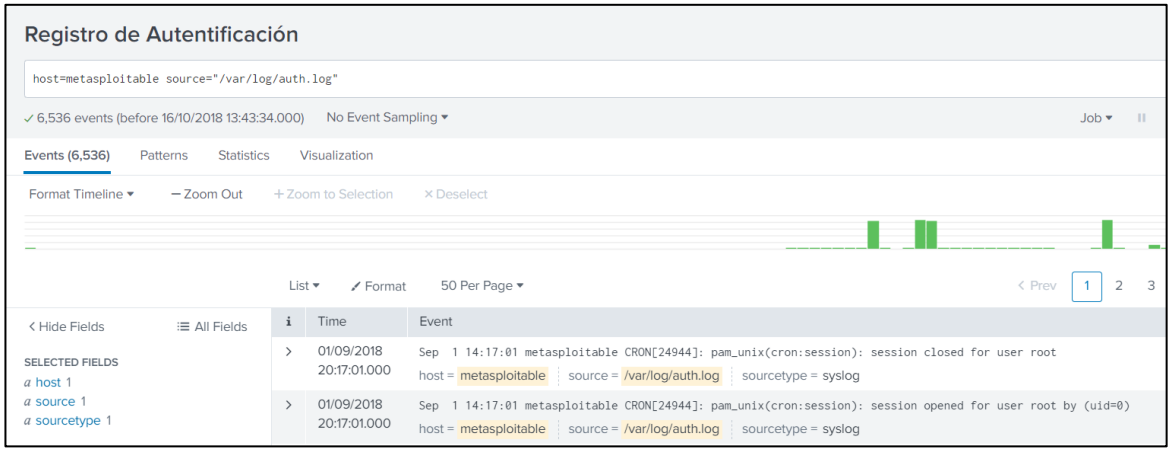


Ilustración 86: Resultados de la búsqueda que hemos configurado en el apartado anterior

Y también hemos configurado que se añada un enlace a la configuración de la alerta, a la que podremos acceder si hacemos clic en el nombre de esta que aparece en el email.

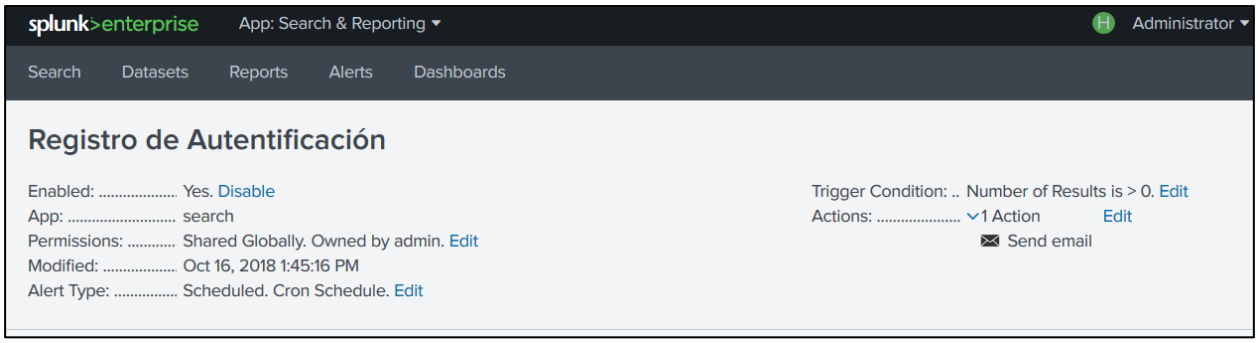


Ilustración 87: Configuración de la alerta

Aparte de visualizar las alertas que configuremos, Splunk nos ofrece Datasets [47] y Dashboards [48] configurables para visualizar la información que consideremos importante de un solo vistazo, ya sea en forma de logs con los Datasets o con gráficas y paneles gracias a los Dashboards, como el que hemos configurado para la vista de vulnerabilidades en la ilustración 42 .

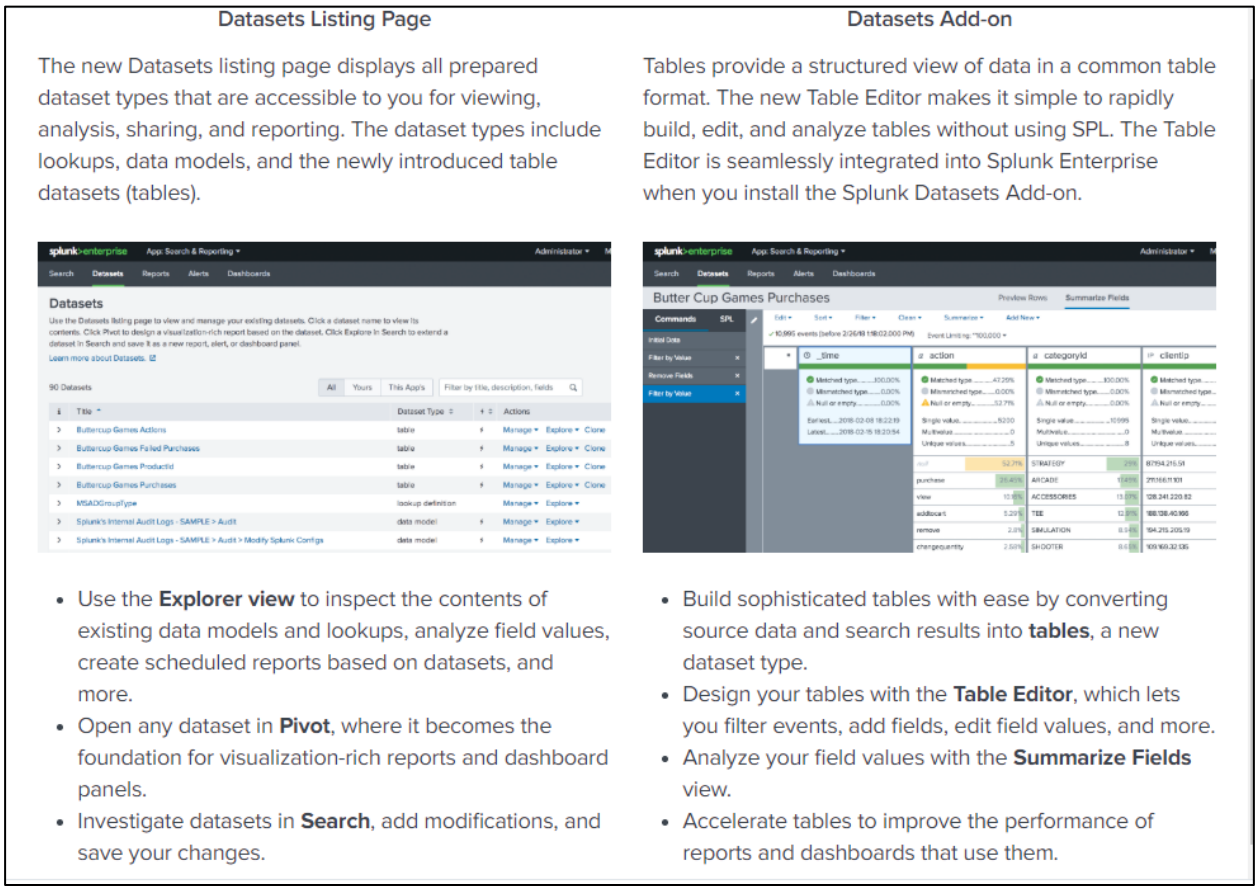


Ilustración 88: Posibles configuraciones para los Datasets

3.8 Remediación.

En el caso de la vulnerabilidad que estamos detallando sería fácil solucionar el problema: simplemente deberíamos poner una contraseña en los servicios que hemos encontrado que no requieren autenticación para ser usados.

A partir de aquí deberíamos de seguir el ciclo mencionado en la ilustración 10:

Ilustración 9: Ciclo de la gestión de vulnerabilidades

Este proceso es cíclico: Una vez solventada la vulnerabilidad que estábamos tratando, deberíamos validar que se ha remediado el problema con la intervención que hemos realizado y empezar de nuevo el ciclo.

El caso de uso que hemos configurado seguiría siendo válido, dado que, aunque ahora tengamos contraseña, estos servicios pueden ser usados de forma maliciosa, por lo que registrar la actividad de inicios de sesión en la red empresarial debería de seguir siendo prioritario. Sin embargo, sí que podríamos realizar un análisis y ver como afinar las alertas que recibimos de Splunk para que no detecten todos los inicios de sesión, si no los que creamos que pueden ser maliciosos, por ejemplo:

- Si nos encontramos con múltiples intentos de inicio de sesión fallido podríamos encontrarnos ante un ataque de fuerza bruta (probando múltiples combinaciones hasta encontrar aquella que permite el acceso) [49].
- Detectar inicios de sesión desde IPs no autorizadas hacia máquinas monitorizadas por que incluyan información sensible o procesos que puedan afectar a la operativa de la empresa.
- Inicios de sesión fuera de horario de trabajo que pueden indicar una actividad maliciosa.

Y así seguiríamos el ciclo, configurando las nuevas alertas, etc.

4 CONCLUSIONES

"Podemos cambiar, pero nadie puede obligarnos a hacerlo. El cambio suele ocurrir cuando enfrentamos una verdad incuestionable, algo que nos obliga a revisar nuestras creencias."

Isabel Allende

Por desgracia, la gestión de vulnerabilidades es un ciclo sin fin. La seguridad absoluta no es posible, dado que siempre nos encontraremos con nuevas amenazas que puedan poner en peligro los datos o el desarrollo del trabajo de nuestra organización.

Los ciberataques crecen exponencialmente. Citando a importantes medios de comunicación: *España ha batido este año su récord en ciberataques: 120.000 incidentes en 2017 [50]. Se prevé que el coste de los ciberataques para las empresas en 2020 supere los 150 billones de dólares [51]*

Hoy en día vemos como cada vez tenemos más ataques de *"día Zero"* [52], en los que se incluyen vulnerabilidades en el propio código de las aplicaciones que aún no han sido publicadas por el proveedor, o como los hackeos a organizaciones para la sustracción de datos o para ataques de denegación de servicio [53] son cada vez más frecuentes.

Además, nos encontramos con que los gobiernos intentan proteger cada vez más los datos de la amenaza del robo de datos cibernético: la GDPR (Reglamento General de Protección de Datos) que entró en vigor el 25 de mayo de 2018 pretende hacer responsables a las empresas de implementar medidas efectivas para la protección de los datos personales de los usuarios. El no cumplimiento de esta ley puede suponer sanciones que pueden llegar hasta los 20 millones de euros.

La ciberseguridad se ha vuelto una necesidad.

Por ello es importante anticiparse, realizar escaneos rutinariamente, sobre todo después de actualizar o modificar los equipos de la compañía, y tener un buen sistema de alertas que detecte actividad maliciosa.

Deberemos realizar un proceso proactivo de defensa ante estas amenazas (T*hreat hunting* [54]*)* y buscar posibles eventos "extraños" que puedan suponer una vulneración de nuestra barrera de seguridad.

Gracias a Nessus y a Splunk podemos optimizar la seguridad de nuestro sistema, así como monitorizar los riesgos que no podamos solventar.

En concreto, destacaremos Splunk: Su extrema versatilidad, tanto a la hora de desplegarlo como a la hora de gestionar las alertas, y las facilidades que aporta a la hora de analizar datos, dado que está considerado una de las mejores herramientas para big data [55], hacen que Splunk cada vez esté destacando más entre sus competidores.

Las empresas que se dedican a la gestión de la seguridad cada vez optan más por cambiar a este SIEM sobre todo para realizar un Threat hunting más exhaustivo [56] dada la amplia posibilidad de indexación y búsqueda de datos que ofrece.

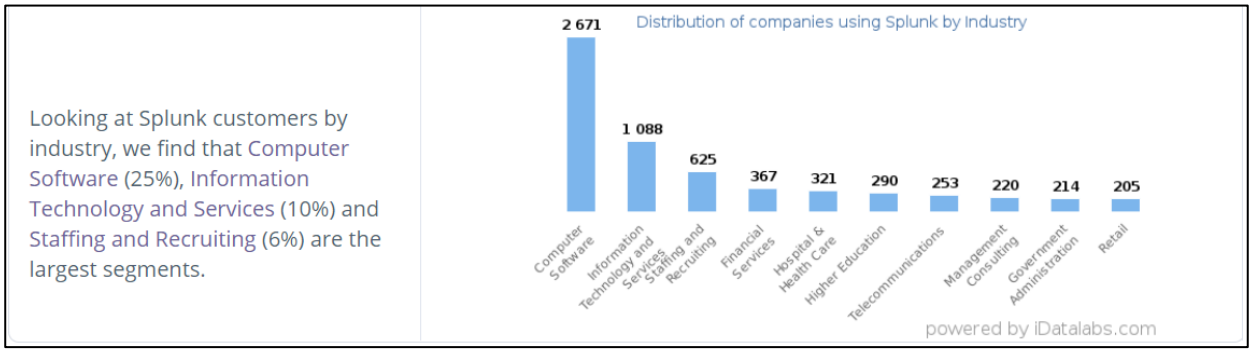


Ilustración 89: Industrias que más usan Splunk [57]

Por ello, nosotros hemos contado con Nessus para ayudarnos a gestionar las vulnerabilidades de forma eficiente, y con Splunk para gestionar la seguridad de nuestra empresa.

De esta forma, aunque la seguridad absoluta no sea posible, contaremos con la forma de prevenir los ataques, así como de detectar intrusos y recopilar información sobre ellos o los datos a los que acceden.

REFERENCIAS

[1] Wikipedia, «Red de ordenadores,» [En línea]. Available: https://es.wikipedia.org/wiki/Red_de_computadoras.

[2] Wikipedia, «Seguridad Informatica,» [En línea]. Available: https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica.

[3] Incibe, «Diferencias entre Vulnerabilidad y Amenaza,» [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

[4] Wikipedia, «Hacker,» [En línea]. Available: https://es.wikipedia.org/wiki/Hacker_(seguridad_inform%C3%A1tica).

[5] Wkipedia, «Ciberataque,» [En línea]. Available: https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico.

[6] Wikipedia, «Log,» [En línea]. Available: https://es.wikipedia.org/wiki/Log_(inform%C3%A1tica).

[7] Wikipedia, «SIEM,» [En línea]. Available: https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_eventos_e_informaci%C3%B3n_de_seguridad.

[8] Wikipedia, «Certificado,» [En línea]. Available: https://es.wikipedia.org/wiki/Certificado_digital.

[9] Wikipedia, «Norma,» [En línea]. Available: https://es.wikipedia.org/wiki/Norma_(tecnolog%C3%ADa).

[10] tuxotron, «Técnicas de Pivoting,» [En línea]. Available: https://www.cyberhades.com/2017/03/26/tecnicas-pivote-atacantes/.

[11] A. Kondratenko, «A Red Teamer's guide to pivoting,» [En línea]. Available: https://artkond.com/2017/03/23/pivoting-guide/.

[12] Tenable, «Nessus by Tenable,» [En línea]. Available: https://www.tenable.com/products/nessus/nessus-professional.

[13] Gartner, «About Gartner,» [En línea]. Available: https://www.gartner.com/en/about.

[14] Sólo pienso en T!c, «Entender el cuadrante mágico de Gartner,» 2016. [En línea]. Available: http://www.solopiensoentic.com/cuadrante-magico-de-gartner/.

[15] Gartner, «Comparativa de los siems según Gartner,» 2018. [En línea]. Available: https://www.gartner.com/reviews/customer-choice-awards/security-information-event-management.

[16] K. Scarfone, «Caracteristicas a tener en cuenta en un siem,» [En línea]. Available: https://searchsecurity.techtarget.com/feature/Comparing-the-best-SIEM-systems-on-the-market.

[17] Gartner, «Splunk contra los lideres,» [En línea]. Available: https://www.gartner.com/reviews/market/security-information-event-management/compare/splunk-vs-ibm-vs-logrhythm-vs-mcafee.

[18] Gartner, «Types of forwarders,» [En línea]. Available: http://docs.splunk.com/Documentation/Splunk/7.1.2/Forwarding/Typesofforwarders.

[19] Gartner, «Comparación entre los lideres,» [En línea]. Available: https://www.gartner.com/reviews/market/vulnerability-assessment/compare/tenable-vs-qualys-vs-rapid7.

[20] Wikipedia, «Nmap,» [En línea]. Available: https://es.wikipedia.org/wiki/Nmap.

[21] Tenable, «Compare Tenable with industry vulnerability management solutions,» [En línea]. Available: https://www.tenable.com/products/competitive-comparison.

[22] trustradius, «trustradius,» [En línea]. Available: https://www.trustradius.com/compare-products/rapid7-nexpose-vs-tenable-securitycenter.

[23] Gbadvisors, «Comparación entre escaneres,» 2017. [En línea]. Available: http://www.gb-advisors.com/comparison-tenable-io-vs-qualysguard-vs-rapid7/.

[24] Capterra, «Capterra,» [En línea]. Available: https://www.capterra.es/software/130577/nessus.

[25] Tenable, «Pricing of Nessus,» [En línea]. Available: https://store.tenable.com/1479/?scope=checkout&cart=192368&quantity=1&currency=USD&country=US&cfg=tenable_swapify&showpricescale=false.

[26] Search Security, «Comparing the best SIEM systems on the market,» [En línea]. Available: https://searchsecurity.techtarget.com/feature/Comparing-the-best-SIEM-systems-on-the-market.

[27] Gartner, «SIEMs at Gartner,» [En línea]. Available: https://www.gartner.com/reviews/market/security-information-event-management.

[28] Trustwave, «Threat Detection,» [En línea]. Available: https://www.trustwave.com/en-us/services/managed-security/threat-detection/.

[29] Wikipedia, «MSSP,» [En línea]. Available: https://en.wikipedia.org/wiki/Managed_security_service.

[30] idatalabs, «Splunk stadistics in compaanies,» [En línea]. Available: https://idatalabs.com/tech/products/splunk.

[31] Splunk, «Splunk como lider en el cuadrante de Gartner,» [En línea]. Available: https://www.splunk.com/blog/2017/12/07/splunk-named-a-leader-in-gartner-siem-magic-quadrant-for-the-fifth-straight-year.html.

[32] Gartner, «Reseñas de los consumidores,» [En línea]. Available: https://www.gartner.com/reviews/customers-choice/security-information-event-management.

[33] Wikipedia, «Wikipedia sobre Splunk,» [En línea]. Available: https://en.wikipedia.org/wiki/Splunk.

[34] Splunk, «Características de Splunk Lights y diferencias con Enterprise,» [En línea]. Available: https://www.splunk.com/pdfs/technical-briefs/splunk-light-tech-brief.pdf.

[35] Splunk, «Splunk Cloud,» [En línea]. Available: https://www.splunk.com/es_es/products/splunk-cloud.html.

[36] Splunk, «Splunk Enterprise,» [En línea]. Available: https://www.splunk.com/es_es/products/splunk-enterprise.html.

[37] Splunk, «Deployment Server,» [En línea]. Available: http://docs.splunk.com/Documentation/Splunk/7.1.2/Updating/Deploymentserverarchitecture.

[38] Splunk, «Resumen Splunk Enterprise,» [En línea]. Available: https://www.splunk.com/pdfs/product-briefs/splunk-enterprise.pdf.

[39] Search Security, «Splunk Enterprise Security: Product overview,» [En línea]. Available: https://searchsecurity.techtarget.com/feature/Splunk-Enterprise-Security-Product-overview.

[40] Wikipedia, «Sistema redundante,» [En línea]. Available: https://es.wikipedia.org/wiki/Sistema_redundante.

[41] Globalsign, «Globalsign,» [En línea]. Available: https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/.

[42] Knowledge, «How to locate the serial number of an SSL certificate,» [En línea]. Available: https://knowledge.digicert.com/solution/SO25517.html.

[43] jellingwood, « How To Monitor System Authentication Logs on Ubuntu,» [En línea]. Available: https://www.digitalocean.com/community/tutorials/how-to-monitor-system-authentication-logs-on-ubuntu.

[44] Splunk, «The Splunk REST API,» [En línea]. Available: http://dev.splunk.com/restapi.

[45] Splunk, «Use cron expressions for alert scheduling,» [En línea]. Available: http://docs.splunk.com/Documentation/Splunk/7.1.2/Alert/CronExpressions.

[46] Adictosaltrabajo, «Expresiones CRON,» [En línea]. Available: https://www.adictosaltrabajo.com/2010/02/22/expresiones-cron/.

[47] Splunk, «Datasets,» [En línea]. Available: https://docs.splunk.com/Documentation/Splunk/7.1.2/Knowledge/Aboutdatasets.

[48] Splunk, «About Dashboards,» [En línea]. Available: http://docs.splunk.com/Documentation/Splunk/7.1.2/SearchTutorial/Aboutdashboards.

[49] Wikipedia, «Ataque de fuerza bruta,» [En línea]. Available: https://es.wikipedia.org/wiki/Ataque_de_fuerza_bruta.

[50] ABC, «España bate su récord en ciberataques: 120.000 incidentes en 2017,» [En línea]. Available: https://www.abc.es/tecnologia/informatica/abci-espana-bate-record-ciberataques-120000-incidentes-2017-201801111645_noticia.html.

[51] Cybintsolutions, «13 Alarming Cyber Security Facts and Stats,» [En línea]. Available: https://www.cybintsolutions.com/cyber-security-facts-stats/.

[52] Wikipedia, «Ataque de día cero,» [En línea]. Available: https://es.wikipedia.org/wiki/Ataque_de_d%C3%ADa_cero.

[53] Wikipedia, «Ataque de denegación de servicio,» [En línea]. Available: https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio.

[54] Wikipedia, «Threat hunting,» [En línea]. Available: https://en.wikipedia.org/wiki/Cyber_threat_hunting.

[55] Splunk, «Splunk en Big Data,» [En línea]. Available: https://www.splunk.com/es_es/solutions/solution-areas/big-data.html.

[56] Splunk, «Uso de Splunk para Threat Hunting,» [En línea]. Available: https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html.

[57] idatalabs, «Splunk en la industria,» [En línea]. Available: https://idatalabs.com/tech/products/splunk.

[58] A. Kondratenko, «A Red Teamer's guide to pivoting,» [En línea]. Available: https://artkond.com/2017/03/23/pivoting-guide/.

[59] Wikipedia, «Función hash,» [En línea]. Available: https://es.wikipedia.org/wiki/Funci%C3%B3n_hash.

[60] Wikipedia, «MD5,» [En línea]. Available: https://es.wikipedia.org/wiki/MD5.

[61] IBM, «Datos para la solicitud de la versión de prueba,» [En línea]. Available: https://www.ibm.com/account/reg/es-es/signup?formid=urx-30590.