Práctica del Tema 5

En esta práctica se pretende que el estudiante sea capaz de instalar y configurar un SIEM simple y probar las diferentes herramientas de las que dispone. Para ello es necesario que se haga primero una revisión de las alternativas existentes y luego se instale aquél SIEM que puede ser más interesante (o el que recomienda el equipo docente: Security Onion)

La práctica está compuesta por dos partes, cuyos entregables se añadirán a un fichero zip completo. Cada parte tendrá un directorio denominado parteX (X en el rango [1:2]), que deberá contener los entregables que se piden para cada parte/apartado.

Parte 1. Selección de un SIEM Open Source (3 puntos)

En esta primera parte el estudiante debe hacer un análisis de las diferentes soluciones de tipo SIEM que hay en el mercado, incluyendo versiones comerciales y Open Source. Se pueden usar diferentes fuentes de información (referenciándolas en el informe). A modo de ejemplo, aquí se presentan unas referencias concretas sobre plataformas SIEM de tipo Open Source:

https://solutionsreview.com/security-information-event-management/the-10-best-open-source-siem-tools-for-businesses/

https://www.dnsstuff.com/free-siem-tools

https://logdna.com/open-source-siem-tools/

Se deben seleccionar 5 de tipo comercial y 5 de tipo Open Source, y se deben revisar las características de cada una de ellas, indicando en una tabla para cada SIEM sus ventajas e inconvenientes más importantes. Aquí se debe detallar, si es posible, la versión actual y la fecha de dicha versión.

Entregables del apartado

Se debe incluir en el subdirectorio “parte1” del fichero zip los siguientes apartados:

- Subdirectorio **doc** (dentro del directorio parte1). Informe de análisis y comparativa (no más de 10 páginas) con las diferentes alternativas SIEMS actualizadas.

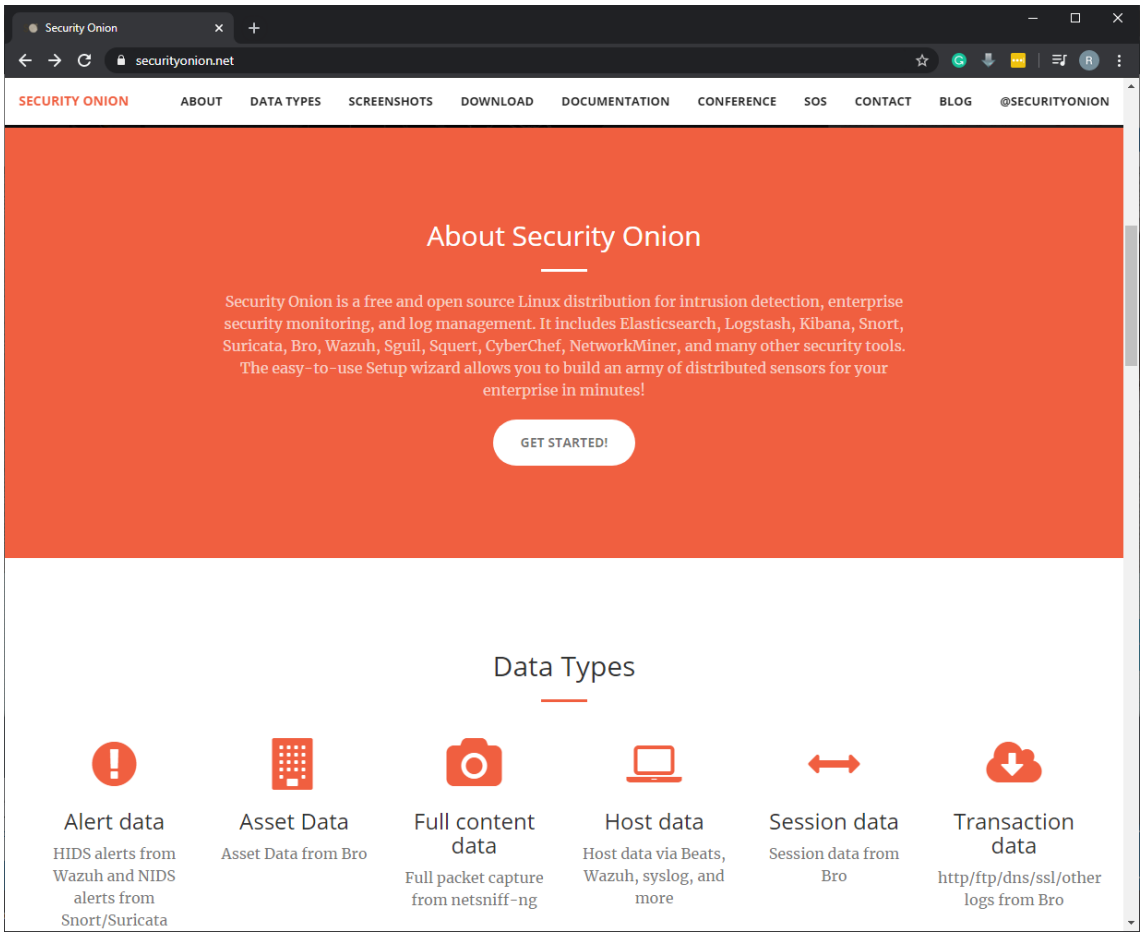
Se valorará la capacidad de síntesis y la claridad de la información proporcionada en el informe.

Parte 2. Instalación del SIEM (7 puntos)

Se debe seleccionar uno de los SIEMS analizados en el apartado anterior y desplegar la solución en un entorno de producción. Este entorno puede ser un entorno local (usando máquinas virtuales o contenedores) o un entorno en la nube. Para implementar el entorno en la nube, se proporcionará al estudiante un acceso a AWS para la creación de instancias EC2 configurables que permitan el despliegue de la solución SIEM.

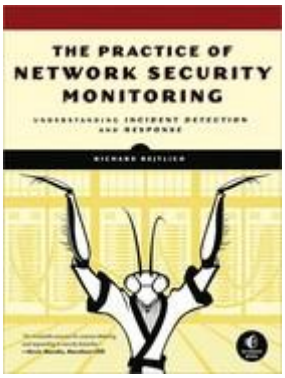
En el curso virtual se han añadido videos específicos asociados al registro y uso del programa AWSEducate (https://www.awseducate.com/) que es la herramienta que se usará para poder usar los créditos en dólares que se han asociado a cada cuenta AWS que se asignará al estudiante (no es necesario que el estudiante proporcione ninguna información de la tarjeta de crédito pero debe entrar a través de AWSEducate a su portal de servicios AWS).

Si no se dispone de una información clara o adecuada para el despliegue del SIEM seleccionado se debe indicar en el informe de pruebas porque esto es así. En cualquier caso si no se tiene claro que SIEM configurar, el equipo docente recomienda SecurityOnion:



https://securityonion.net/

En el libro de referencia “The Practice of Network Security Monitoring” hay tres capítulos específicos donde se detallan los procedimientos de instalación en modo simple y en modo de producción

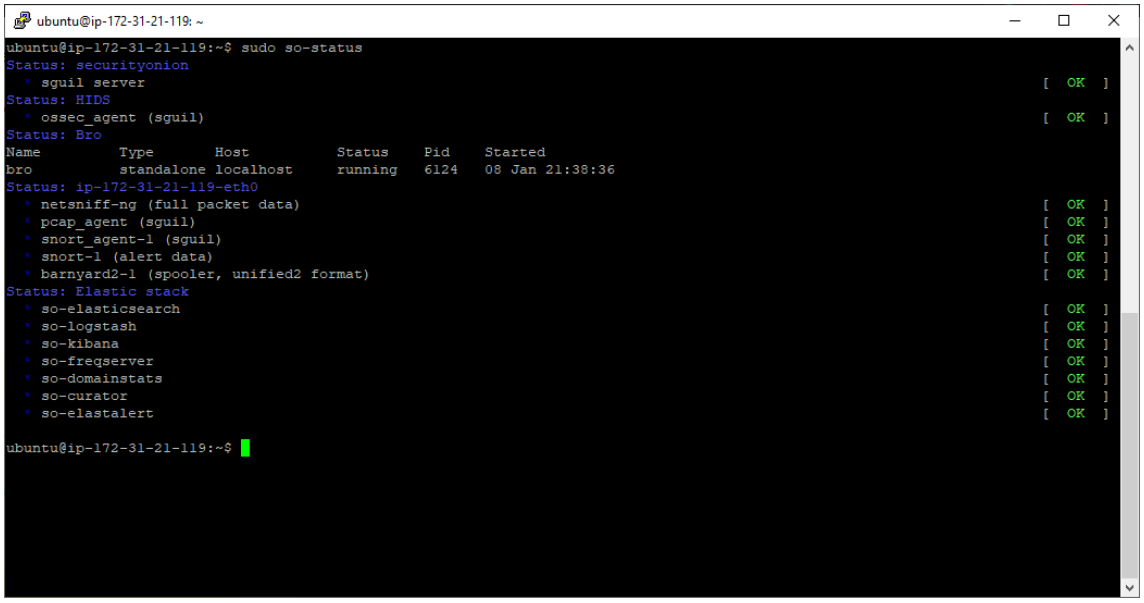


II. Security Onion Deployment

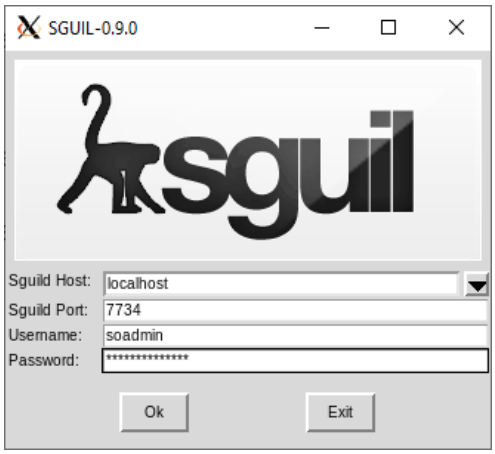
Para usarlo en la nube de AWS se recomienda usar una instancia EC2 adecuada con la versión de Ubuntu 16.04 (la última soportada por SecurityOnion) y seguir los pasos indicados aquí:

https://securityonion.readthedocs.io/en/latest/installing-on-ubuntu.html

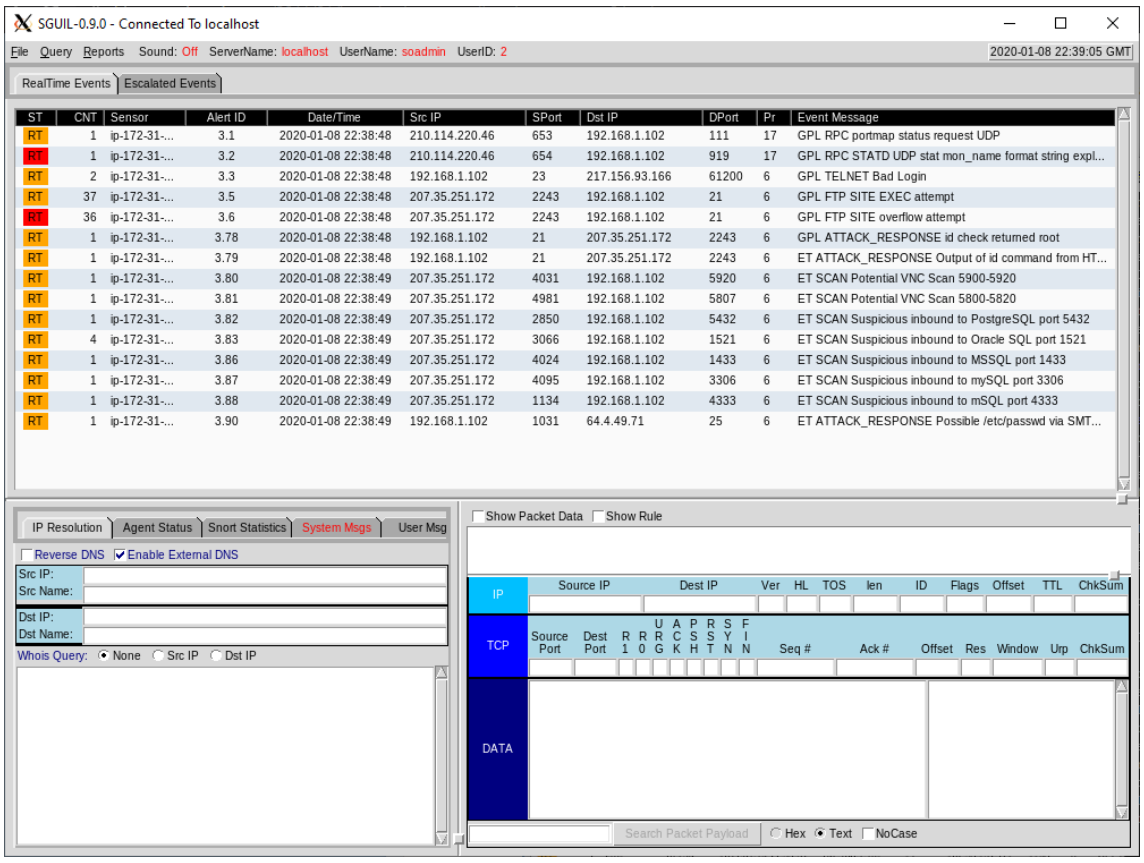
Se recomienda usar una instancia de tipo t2.xlarge (para poder ejecutar ElasticSearch) y al menos 100 GB de disco (realmente serían necesarios más, pero solo se está evaluando este SIEM). Una vez instalado, se deben poder probar las diferentes herramientas y tener evidencias de la instalación con éxito de SecurityOnion. A continuación se muestran algunas de estas evidencias:



Security Onion status en la instancia EC2



Conexión a Sguil usando el script sguil.tk



Cliente Sguil mostrando unas alertas simuladas

Para el caso de SecurityOnion, la lista de herramientas disponibles son las siguientes:

https://securityonion.readthedocs.io/en/latest/tools.html

Se deben poder dar evidencias de muchas de ellas, y en algún caso (como el anterior en Sguil) se pueden simular alertas mediante el uso de herramientas alternativas (como tcpreplay).

Entregables del apartado

Se debe incluir en el subdirectorio “parte2” del fichero zip con la solución completa, los siguientes apartados:

- Subdirectorio **doc** (dentro del directorio parte2). Indicar en un informe de no más de dos páginas los problemas encontrados en la instalación del SIEM seleccionado.

- Subdirectorio **despliegue** (dentro del directorio parte2). Se añadirá un documento con los pasos de instalación seguidos (simplificado) asi como las evidencias necesarias del despliegue exitoso: local (Docker files, Imágenes de funcionamiento activo de las herramientas disponibles, Plantillas de VM, etc,) o en la nube (IPs/DNs públicos disponibles en la nube y enlaces a las diferentes herramientas disponibles en el SIEM).

Se valorará el despliegue en la nube por encima de una instalación local y el número de herramientas disponibles en el SIEM. También se tendrá en cuenta el formato de instalación distribuido, donde los diferentes componentes se instalen en diferentes ubicaciones (máquinas virtuales, contendores Docker, instancias EC2, etc.). Estas instalaciones tendrán una mejor evaluación que el resto (por ejemplo, usar la forma de instalación distribuida de SecurityOnion).