

Documentación del Blockchain	2
Introducción.....	2
Funcionalidades	2
Login y creación de usuario	2
Consulta de saldo.....	3
Consulta de transacciones	3
Generar transacción	4
Configuración del Blockchain.....	4
Backend y base de datos	4
Documentación de Snort, Snorby y Zabbix	5
Snort.....	5
Introducción.....	5
Instalación y Configuración.....	5
Paso a paso	5
Uso básico	6
Snorby	7
Introducción.....	7
Instalación y Configuración.....	7
Uso básico	7
Paso a paso	7
Zabbix.....	10
Introducción.....	10
Instalación y Configuración.....	10
Uso básico	10
Monitoreo y análisis de tráfico	11

Documentación del Blockchain

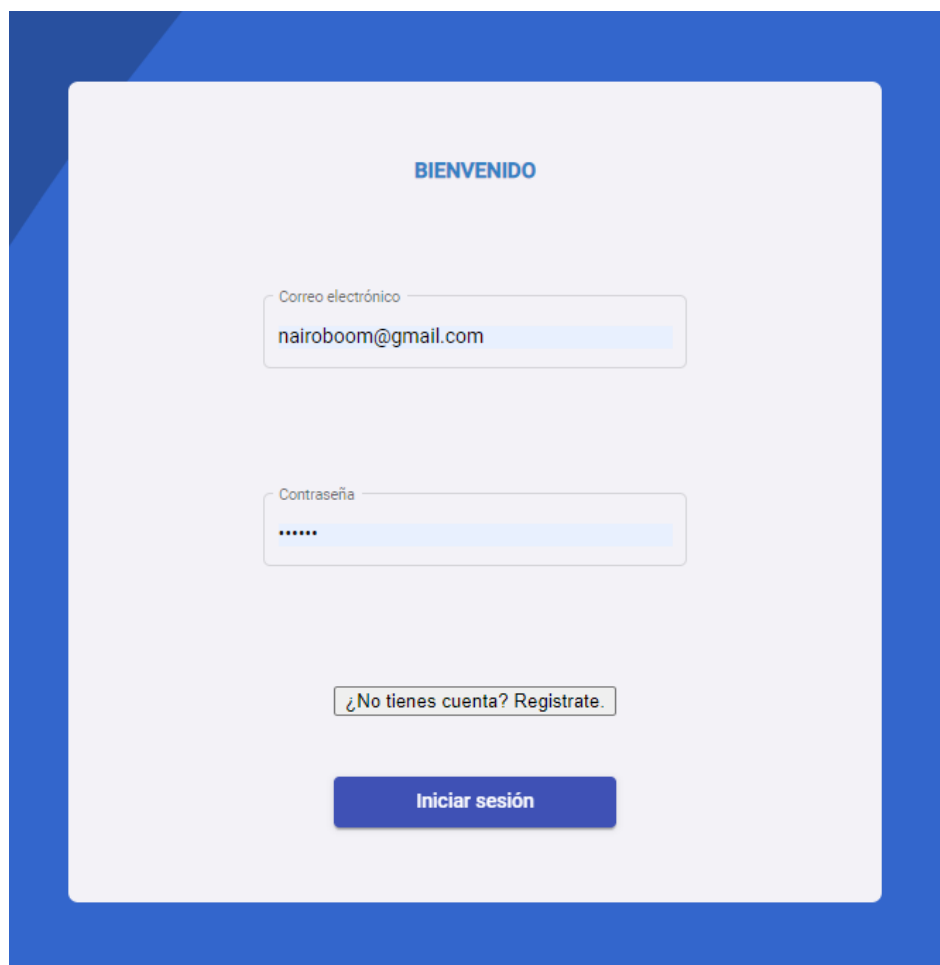
Introducción

El Blockchain es una tecnología de registro distribuido que permite la creación y el mantenimiento de una base de datos segura y transparente. En este documento, se describe el Blockchain desarrollado en Python para el backend y Angular para el frontend, con una base de datos SQL Server.

Funcionalidades

Login y creación de usuario

El Blockchain cuenta con un sistema de autenticación que permite a los usuarios registrarse y acceder a sus cuentas. Para iniciar sesión, el usuario deberá proporcionar su nombre de usuario y contraseña. En caso de no tener una cuenta, se le proporcionará la opción de crear una nueva.

A login form interface with a blue header and footer. The form is centered on a light gray background. It features a 'BIENVENIDO' heading, two input fields for 'Correo electrónico' (containing 'nairoboom@gmail.com') and 'Contraseña' (masked with dots), a link for '¿No tienes cuenta? Regístrate.', and a blue 'Iniciar sesión' button.

BIENVENIDO

Correo electrónico

nairoboom@gmail.com

Contraseña

[¿No tienes cuenta? Regístrate.](#)

Iniciar sesión

REGISTRO

Correo electrónico

Nombre

Apellido

Cedula

Contraseña

Crear cuenta

Iniciar sesión

Consulta de saldo

Una vez que el usuario haya iniciado sesión, podrá realizar consultas sobre su saldo actual en la plataforma. El saldo representa la cantidad de fondos disponibles en la cuenta del usuario en el Blockchain.

Saldo de mi cartera

Tu saldo es: \$900.00

Generar transacción

Consultar transacciones

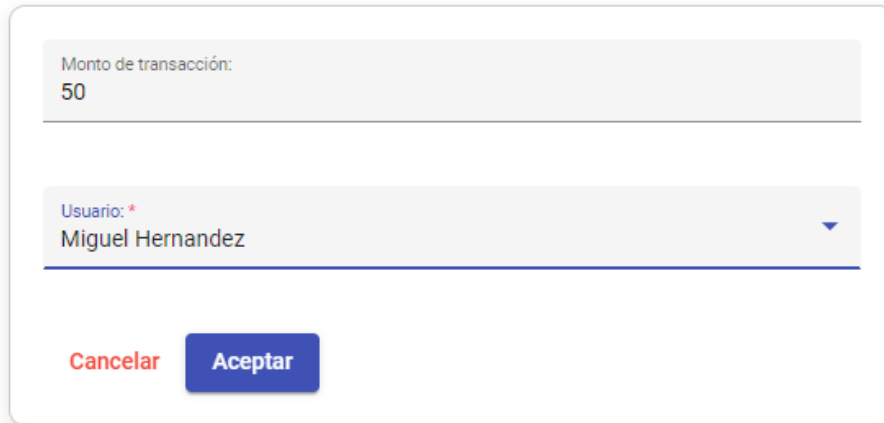
Consulta de transacciones

El Blockchain también ofrece la funcionalidad de consultar las transacciones realizadas por el usuario. Estas transacciones incluyen tanto los envíos como las recepciones de fondos. Cada transacción mostrará la fecha, el monto y los detalles de la operación.

Consultas Transacción				
Fecha	Monto	Usuario		
29/05/2023	-100	mateo		

Generar transacción

El usuario podrá generar nuevas transacciones a través del Blockchain. Al seleccionar esta opción, se le pedirá que indique el monto de la transacción que desea realizar. El sistema verificará si el usuario tiene fondos suficientes y le mostrará una lista de usuarios registrados en el sistema para seleccionar al destinatario de la transacción.



Formulario para generar una transacción. El formulario tiene un campo de texto para el monto de la transacción, un campo de selección para el usuario, y dos botones: 'Cancelar' y 'Aceptar'.

Monto de transacción:
50

Usuario: *
Miguel Hernandez

Cancelar Aceptar

Configuración del Blockchain

El Blockchain está configurado utilizando Docker, lo que facilita su implementación y despliegue. A continuación, se muestran las líneas de código del archivo **docker-compose.yml** para cada uno de los servicios involucrados:

Backend y base de datos

```
version: "3.9"
services:
  midb:
    image: mateofuentes/bd_block:v1
    ports:
      - "1433:1433"
    networks:
      - red_block

  miback:
    image: mateofuentes/app_back:v1
    ports:
      - "5000:5000"
    networks:
      - red_block
    depends_on:
      - midb

  mifront:
    image: miguelhernandezdev/mifront:v1
    ports:
      - "4200:4200"
    networks:
      - red_block
    depends_on:
      - miback

networks:
  red_block:
    driver: bridge
    ipam:
      driver: default
      config:
        - subnet: 172.16.0.0/24
          gateway: 172.16.0.1
          ip_range: 172.16.0.0/24
```

En el bloque de código anterior, se definen tres servicios: **midb**, **miback** y **mifront**. El servicio **midb** representa la base de datos SQL Server utilizada por el backend. El servicio **miback** representa el backend desarrollado en Python y el servicio **mifront** representa el frontend desarrollado en Angular. Cada servicio se configura con sus respectivos puertos y dependencias.

Documentación de Snort, Snorby y Zabbix

Snort

Introducción

Snort es un sistema de detección y prevención de intrusiones de código abierto. Se utiliza para monitorear y analizar el tráfico de red en busca de posibles amenazas y ataques. Esta documentación proporciona una visión general de Snort y los pasos básicos para su configuración y uso.

Instalación y Configuración

- **Descarga de Snort:** Visita el sitio web oficial de Snort y descarga la última versión estable de Snort para tu sistema operativo.
- **Instalación de dependencias:** Asegúrate de tener las dependencias necesarias, como libpcap, libdnet y libpcrc, instaladas en tu sistema.
- **Configuración del archivo de reglas:** Crea un archivo de reglas personalizado o utiliza reglas predefinidas disponibles en línea. Especifica los patrones y comportamientos que Snort buscará en el tráfico de red.
- **Configuración de Snort:** Crea un archivo de configuración de Snort (snort.conf) donde se especifiquen las opciones y ajustes necesarios. Incluye la ubicación del archivo de reglas y la interfaz de red que Snort debe monitorear.
- **Ejecución de Snort:** Utiliza el comando `snort -c snort.conf -i <interfaz>` para iniciar Snort. Reemplaza <interfaz> con el nombre de la interfaz de red que deseas monitorear.

Paso a paso

- 1. Actualiza los repositorios del sistema:**
 - `sudo apt update`
- 2. Instala las dependencias necesarias:**
 - `sudo apt install -y build-essential libpcap-dev libpcrc3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev ethtool`
- 3. Descarga el código fuente de Snort desde el sitio oficial:**
 - `wget https://www.snort.org/downloads/snort/snort-<version>.tar.gz`
 - Reemplaza <version> con la versión deseada.
- 4. Extrae el archivo comprimido:**
 - `tar -xvf snort-<version>.tar.gz`
- 5. Navega al directorio del código fuente de Snort:**
 - `cd snort-<version>`
- 6. Configura y compila Snort:**

- ./configure --enable-sourcefire
 - make sudo
 - make install
- 7. Crea el directorio para los archivos de configuración:**
 - sudo mkdir /etc/snort
 - 8. Copia los archivos de configuración predeterminados al directorio creado:**
 - sudo cp etc/* /etc/snort/
 - 9. Descarga las reglas actualizadas de Snort:**
 - sudo wget https://www.snort.org/downloads/community/community-rules.tar.gz
 - 10. Extrae las reglas descargadas:**
 - sudo tar -xvf community-rules.tar.gz -C /etc/snort/rules
 - 11. Configura la interfaz de red en la que Snort debe monitorear el tráfico:**
 - sudo vi /etc/snort/snort.conf
 - 12. Inicia Snort para probar su funcionamiento:**
 - sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf

Esto iniciará Snort en modo consola con la configuración especificada.

```

2023-05-29 16:51:48
2023-05-29 16:51:48      --== Initialization Complete ==--
2023-05-29 16:51:48
2023-05-29 16:51:48      -*> Snort! <*-
2023-05-29 16:51:48      o" )~ Version 2.9.9.0 GRE (Build 56)
2023-05-29 16:51:48      '"" By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
2023-05-29 16:51:48      Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
2023-05-29 16:51:48      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
2023-05-29 16:51:48      Using libpcap version 1.7.4
2023-05-29 16:51:48      Using PCRE version: 8.38 2015-11-23
2023-05-29 16:51:48      Using ZLIB version: 1.2.8
2023-05-29 16:51:48
2023-05-29 16:51:48      Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_DNS Version 1.1 <Build 4>
2023-05-29 16:51:48      Preprocessor Object: SF_SDF Version 1.1 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_POP Version 1.0 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_SMTTP Version 1.1 <Build 9>
2023-05-29 16:51:48      Preprocessor Object: SF_SSH Version 1.1 <Build 3>
2023-05-29 16:51:48      Preprocessor Object: SF_SIP Version 1.1 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
2023-05-29 16:51:48      Preprocessor Object: SF_GTP Version 1.1 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
2023-05-29 16:51:48      Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
2023-05-29 16:51:48      Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
2023-05-29 16:51:48 Commencing packet processing (pid=69)

```

Uso básico

- Monitoreo de eventos: Snort comenzará a monitorear el tráfico en la interfaz especificada y generará eventos cuando detecte posibles amenazas o actividades sospechosas. Puedes ver los eventos en tiempo real o almacenarlos en un archivo de registro para su posterior análisis.

Snorby

Introducción

Snorby es una interfaz web que proporciona una plataforma para administrar y analizar los eventos generados por Snort. Permite visualizar, filtrar y analizar los eventos de manera conveniente. Esta documentación te guiará a través de los pasos básicos para la configuración y uso de Snorby.

Instalación y Configuración

- **Descarga de Snorby:** Visita el repositorio de Snorby en GitHub y descarga la última versión estable de Snorby.
- **Configuración de la base de datos:** Instala y configura una base de datos compatible, como MySQL o PostgreSQL, para almacenar los datos de Snorby.
- **Configuración de Snorby:** Copia el archivo de configuración de ejemplo (`snorby_config.yml.example`) y renómbralo como `snorby_config.yml`. Edita este archivo y proporciona los detalles de configuración necesarios, como la información de la base de datos.

Uso básico

- **Inicio de Snorby:** Utiliza el comando `rails server` para iniciar el servidor de Snorby. Esto permitirá el acceso a la interfaz web de Snorby.
- **Acceso a la interfaz web:** Abre un navegador web y navega a la dirección `http://localhost:3000` (o la dirección correspondiente si has configurado un puerto diferente). Esto te llevará a la interfaz de usuario de Snorby.
- **Visualización de eventos:** En la interfaz de Snorby, podrás ver una lista de eventos generados por Snort. Utiliza las diferentes opciones de filtrado y búsqueda para explorar y analizar los eventos de manera eficiente.

Paso a paso

1. **Preparación del entorno:**
 - Asegúrate de tener Ruby y Rails instalados en tu sistema. Puedes verificar su presencia ejecutando los siguientes comandos:
 - `ruby -v`
 - `rails -v`
 - Instala las dependencias necesarias, como MySQL o PostgreSQL, y configura una base de datos para Snorby.
2. **Descarga e instala Snorby:**
 - Clona el repositorio de Snorby desde GitHub:
 - `git clone https://github.com/Snorby/snorby.git`
 - Navega al directorio del proyecto Snorby:
 - `cd snorby`
 - Instala las gemas (paquetes de Ruby) requeridas:
 - `bundle install`
 - Copia el archivo de configuración de ejemplo y renómbralo:
 - `cp config/snorby_config.yml.example config/snorby_config.yml`
 - Abre el archivo `snorby_config.yml` y configura la información de la base de datos y otros ajustes según tu entorno.
3. **Configuración adicional:**

- Configura el servidor web para servir la aplicación Snorby. Puedes utilizar Apache o Nginx como servidor web y configurar un proxy inverso hacia Snorby.
- Configura los trabajadores de fondo (background workers) para el procesamiento de tareas en segundo plano de Snorby. Puedes utilizar herramientas como Sidekiq para esto.

4. Ejecuta Snorby:

- Inicia la aplicación Snorby:
 - rails server
- Accede a Snorby a través de tu navegador web en la dirección **http://localhost:3000** (o la dirección correspondiente según tu configuración).
- Una vez en la dirección, nos aparecerá un login básico para iniciar sesión, ingresamos el usuario correspondiente.

Snorby by threat stack
www.threatstack.com

Login

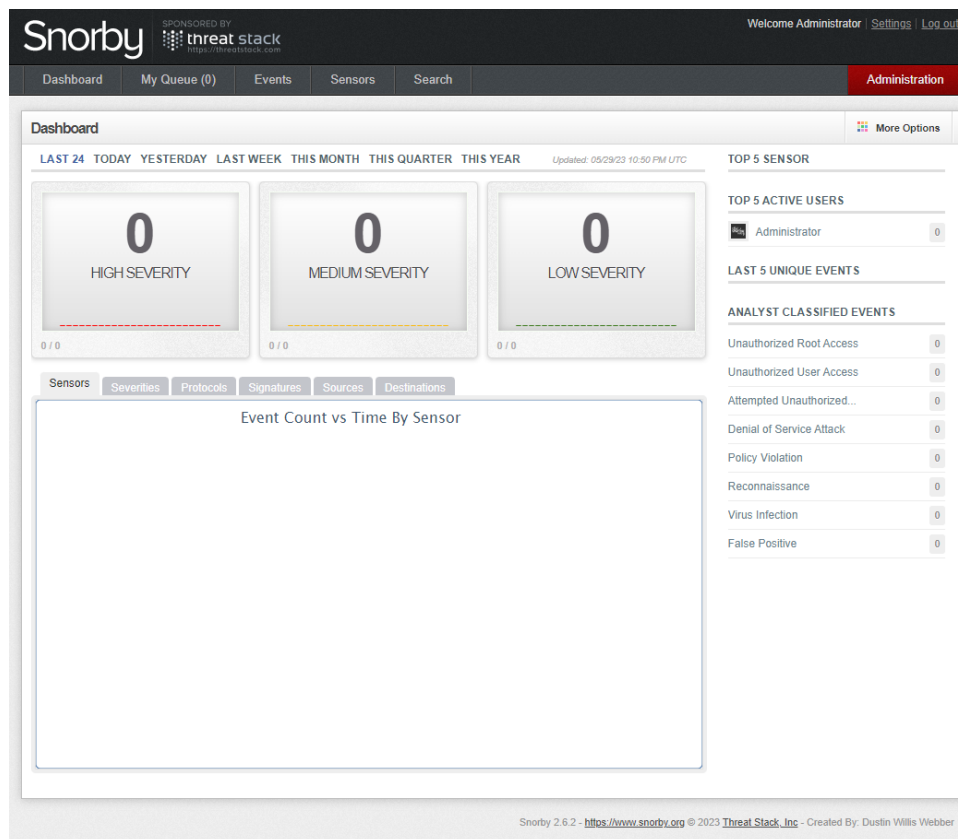
Email
example@example.com

Password
password

Welcome, Sign In Forgot Password? ☒ Remember me

© 2023 Threat Stack, Inc - Created By: Dustin Willis Webber
Snorby 2.6.2 - <https://www.snorby.org>

- Nos aparece el home con un dashboard, el cual contendrá la información de las solicitudes que sean realizadas al blockchain, hay que tener en cuenta, que solo se rastrearán las solicitudes que sean configuradas por medio de las reglas en el snort
- EL Home Dashboard de Snorby es la página principal de la interfaz de usuario de Snorby, donde se muestra un resumen y una visión general de los eventos y actividades de seguridad detectados por Snort. Proporciona una instantánea rápida y fácilmente legible del estado de seguridad de tu red.

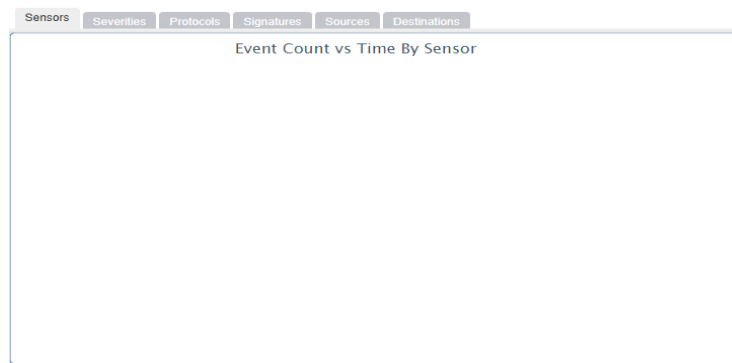


5. Home Dashboard de Snorby suele incluir los siguientes elementos:

- Resumen de eventos: En la parte superior del dashboard, se muestra un resumen de eventos recientes y relevantes, como el número total de eventos, eventos clasificados como ataques, eventos de alta prioridad, etc. Esto te permite tener una idea general de la actividad de seguridad en tu red.



- Gráficos e indicadores: El Home Dashboard puede incluir gráficos y visualizaciones que representan estadísticas y tendencias clave, como el volumen de eventos en el tiempo, los protocolos más frecuentes involucrados en los eventos, los ataques más comunes, etc. Estos gráficos ayudan a identificar patrones y áreas de enfoque.



- Tablas y listas de eventos: Snorby muestra una tabla o lista de eventos recientes, generalmente ordenados por fecha y hora. Esta lista puede incluir detalles como la dirección IP de origen y destino, los protocolos utilizados, las firmas asociadas, la gravedad del evento, etc. Esta información permite un análisis más detallado de los eventos.

Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp	Sessions

- Alertas y notificaciones: Si se han configurado reglas de alerta o umbrales específicos, el Home Dashboard puede mostrar alertas y notificaciones destacadas. Estas alertas pueden indicar eventos críticos o violaciones de seguridad que requieren una atención inmediata.
- Enlaces rápidos: El Home Dashboard puede proporcionar enlaces rápidos a otras secciones importantes de Snorby, como la configuración, los informes generados y las páginas de búsqueda avanzada. Estos enlaces facilitan la navegación y el acceso a funciones adicionales de Snorby.

Zabbix

Introducción

Zabbix es una plataforma de supervisión y registro de red que permite monitorear el estado de los servicios, servidores y hardware de red en tiempo real. Esta documentación proporcionará una descripción general de Zabbix y los pasos básicos para su configuración y uso.

Instalación y Configuración

- Descarga de Zabbix: Visita el sitio web oficial de Zabbix y descarga la última versión estable de Zabbix para tu sistema operativo.
- Configuración del servidor Zabbix: Sigue las instrucciones de instalación proporcionadas en la documentación oficial de Zabbix para configurar y ejecutar el servidor Zabbix. Esto incluye la configuración de la base de datos y la interfaz web de administración.
- Instalación del agente Zabbix: Para monitorear los dispositivos y servicios, instala el agente Zabbix en los sistemas que deseas supervisar. El agente recopilará los datos y los enviará al servidor Zabbix.

Uso básico

- Visualización de datos: Accede a la interfaz web de Zabbix para ver los datos y estadísticas recopilados. Puedes explorar diferentes paneles, gráficos y vistas para obtener información sobre el estado de tus servicios y dispositivos.

- Configuración de alertas: Configura las notificaciones y alertas en Zabbix para recibir avisos cuando se detecten problemas o se superen ciertos umbrales de rendimiento.
- Generación de informes: Utiliza las funciones de generación de informes de Zabbix para obtener informes detallados sobre el rendimiento y la disponibilidad de tus sistemas.

Si queremos omitir los pasos anteriores, simplemente podemos procesar nuestro archivo “docker-compose.yml” con el comando “docker-compose up -d”, ya que en estas imágenes se tiene configurado todo lo necesario para el correcto funcionamiento de ambas herramientas.

Monitoreo y análisis de tráfico

```
version: '3.8'
services:
  db:
    image: mysql
    # NOTE: use of "mysql_native_password" is not recommended: https://dev.mysql.com/doc/mysql-native-password/8.0/en/mysql-native-password.html
    # (this is just an example, not intended to be a production configuration)
    ports:
      - "3306:3306"
    command: [ "mysqld",
      "--default-authentication-plugin=mysql_native_password",
      "--skip-ssl" ]
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: password
      MYSQL_DATABASE: snorby

  adminer:
    image: adminer
    restart: always
    ports:
      - 8080:8080

  snorby:
    image: polinux/snorby
    # NOTE: use of "mysql_native_password" is not recommended: https://dev.mysql.com/doc/mysql-native-password/8.0/en/mysql-native-password.html
    # (this is just an example, not intended to be a production configuration)
    ports:
      - "3000:3000"
    environment:
      - DB_ADDRESS=db
      - DB_USER=root
      - DB_PASS=password
      - OINKCODE=b50b0d83fae4436f24821afd41db163fb23cd7da
    restart: always

  ids:
    image: fabriziogaliano/docker-snort-ids
    network_mode: host
    volumes:
      - "/etc/localtime:/etc/localtime"
      - "/rules:/etc/snort/rules"
      - "/log/snort:/var/log/snort"
      - "/log/barnyard2:/var/log/barnyard2"
    privileged: false
    environment:
      SNORT_NET: "172.16.0.0/24"
      HOST_INT: "eth0"
      HOST_NAME: "snort01"
      PPORK_OINKCODE: "b50b0d83fae4436f24821afd41db163fb23cd7da"
      BARN_DBUSER: "root"
      BARN_DBNAME: "snorby"
      BARN_DBPASS: "password"
      BARN_DBHOST: "10.9.220.209"
    restart: always
```

En el bloque de código anterior, se definen los servicios necesarios para el monitoreo y análisis de tráfico. El servicio **db** representa la base de datos MySQL utilizada por **Snorby**. El servicio **adminer** proporciona una interfaz web para administrar la base de datos. El servicio **snorby** representa la

aplicación **Snorby**, utilizada para el análisis de tráfico y protocolos de red. El servicio ids utiliza la imagen de Docker para **Snort** IDS, que permite la detección y prevención de ciberataques.