



INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 36



09 DE ABRIL DE 2024
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado.....	2
REALIZA UN INFORME SOBRE Data -- Acquisition library (DAQ)	2
¿Qué es la Data Acquisition library (DAQ)?	2
Características principales	2
Como se inicia	3
Funcionalidades de Data Acquisition library (DAQ) para snort	3
Conclusión	4

Enunciado

INDICA SU FUNCIONALIDAD PARA SNORT.-

REALIZA UN INFORME SOBRE Data-- Acquisition library (DAQ) .

¿Qué es la Data Acquisition library (DAQ)?

La biblioteca de Adquisición de Datos, conocida comúnmente como Data Acquisition library (DAQ), es un conjunto de funciones y herramientas diseñadas para facilitar la adquisición de datos desde diferentes dispositivos de medición y sensores. Estas bibliotecas son utilizadas en sistemas de control, automatización industrial, pruebas y mediciones, y otras aplicaciones donde es necesario recopilar datos de sensores y dispositivos de hardware.

La DAQ proporciona una interfaz de programación que permite a los desarrolladores interactuar con dispositivos de adquisición de datos de manera eficiente. Esto incluye la configuración de canales de entrada y salida, la lectura y escritura de datos, el control de la temporización y la sincronización, entre otras funciones.

Características principales

- **Interfaz de programación:** Proporciona una interfaz de programación coherente y fácil de usar para interactuar con los dispositivos de adquisición de datos.
- **Configuración de canales:** Permite configurar los canales de entrada y salida del dispositivo de adquisición de datos, especificando parámetros como el rango de voltaje, la frecuencia de muestreo y la resolución.
- **Lectura y escritura de datos:** Facilita la lectura y escritura de datos desde y hacia los dispositivos de adquisición de datos.
- **Temporización y sincronización:** Permite controlar la temporización y la sincronización de las operaciones de adquisición de datos, garantizando una captura precisa y sincronizada de los datos.
- **Manejo de eventos y notificaciones:** Proporciona capacidades para manejar eventos y notificaciones relacionados con la adquisición de datos, como la llegada de nuevos datos o la ocurrencia de errores.
- **Soporte para múltiples plataformas:** Puede estar disponible para diversas plataformas de hardware y sistemas operativos, como Windows, Linux y sistemas embebidos.
- **Documentación detallada y ejemplos de código:** Ofrece una documentación completa y ejemplos de código para facilitar el desarrollo de aplicaciones utilizando la biblioteca de adquisición de datos.
- **Soporte para diferentes tipos de señales:** Puede admitir una variedad de tipos de señales, como señales analógicas, digitales, de temperatura, de frecuencia, entre otras.
- **Calibración y compensación de señal:** Proporciona funciones para calibrar y compensar las señales medidas, garantizando una precisión y exactitud adecuadas.

- **Compatibilidad con estándares industriales:** Cumple con estándares industriales relevantes en términos de precisión, fiabilidad y seguridad.

Como se inicia

LibDAQ es un proyecto de autotools estándar y se construye e instala como tal:

```
./configure  
make  
make install
```

Si compila desde git, deberá hacer lo siguiente para generar el script de configuración antes de ejecutar los pasos anteriores:

```
./bootstrap
```

Esto construirá e instalará tanto la biblioteca como los módulos.

Cuando se construye la biblioteca DAQ, se generarán versiones estáticas y dinámicas. Los diversos módulos DAQ se construirán si los encabezados y bibliotecas necesarios están disponibles. Puede desactivar módulos individuales, etc. con opciones para configurar.

Para obtener la lista completa de opciones de configuración, ejecute:

```
./configure --help
```

Funcionalidades de Data Acquisition library (DAQ) para snort

Algunas de las funcionalidades que ofrece el DAQ en Snort incluyen:

- **Captura de paquetes:** El DAQ captura los paquetes de red entrantes y salientes que atraviesan la interfaz de red especificada.
- **Soporte para múltiples interfaces:** Puede admitir diferentes interfaces de red, como Ethernet, Wi-Fi, y otros tipos de conexiones de red.
- **Gestión de buffer y almacenamiento temporal:** El DAQ puede gestionar un buffer de paquetes para almacenar temporalmente los paquetes capturados antes de que sean procesados por el motor de reglas de Snort.
- **Filtrado de paquetes:** Permite filtrar los paquetes capturados según criterios específicos, como dirección IP, puerto, protocolo, entre otros, para optimizar el rendimiento y reducir la carga de procesamiento.

- **Integración con el motor de reglas de Snort:** El DAQ proporciona los paquetes capturados al motor de reglas de Snort para su análisis y aplicación de las reglas de detección de intrusiones.
- **Gestión de la configuración:** Facilita la configuración de parámetros relacionados con la captura de paquetes, como el modo de operación, el tamaño del buffer, y otros ajustes de rendimiento.

Conclusión

En conclusión, la Adquisición de Datos (DAQ) es una herramienta esencial en el campo de la instrumentación y el control, que facilita la recopilación de información de sensores y dispositivos de hardware en tiempo real. Esta tecnología ofrece una interfaz de programación coherente y fácil de usar, permitiendo a los desarrolladores interactuar con dispositivos de adquisición de datos de manera eficiente.

Con capacidades para configurar canales, leer y escribir datos, controlar la temporización y sincronización, entre otras funcionalidades, la DAQ es fundamental en una amplia gama de aplicaciones, incluyendo la automatización industrial, las pruebas y mediciones, y el monitoreo en tiempo real. Además, la integración de DAQ con sistemas de detección de intrusiones de red, como en el caso de Snort, demuestra su versatilidad y su importancia en el ámbito de la seguridad informática.