INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 26

20 DE FEBRERO DE 2024

CARLOS DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

INDICA SU FUNCIONALIDAD PARA SNORT .-

--REALIZA UN INFORME SOBRE--Hyperscan--

¿Qué es hyperscan?

Hyperscan es una biblioteca de software de código abierto desarrollada por Intel que se utiliza para realizar búsquedas rápidas y eficientes de patrones en datos.

Está diseñada específicamente para realizar análisis de contenido en tiempo real a gran escala, como la búsqueda de cadenas de texto, expresiones regulares y otros patrones en conjuntos de datos muy grandes, como archivos de registro, paquetes de red, etc.

Características principales

Alto rendimiento: Hyperscan está diseñado para aprovechar al máximo el paralelismo de hardware disponible en las CPUs modernas, utilizando técnicas como el procesamiento en paralelo y la optimización de instrucciones SIMD (Single Instruction, Multiple Data) para lograr un rendimiento óptimo en la búsqueda de patrones.

Soporte para expresiones regulares avanzadas: Hyperscan admite una amplia gama de expresiones regulares, incluidas aquellas que son altamente complejas y que pueden requerir un análisis intensivo para realizar búsquedas eficientes.

Escalabilidad: Hyperscan es capaz de escalar para manejar grandes volúmenes de datos de manera eficiente, lo que lo hace adecuado para aplicaciones que requieren análisis en tiempo real de tráfico de red y otros flujos de datos de alta velocidad.

Bajo consumo de recursos: A pesar de su alto rendimiento, Hyperscan está diseñado para ser eficiente en términos de consumo de recursos, lo que significa que puede ejecutarse en sistemas con recursos limitados sin degradar significativamente el rendimiento.

Requisitos minimos

En hardware

Hyperscan se ejecutará en procesadores x86 en modos de 64 bits (Arquitectura Intel® 64) y 32 bits (Arquitectura IA-32).

Hyperscan es una biblioteca de software de alto rendimiento que aprovecha los avances recientes de la arquitectura Intel. Como mínimo, se requiere compatibilidad con las Extensiones SIMD de transmisión suplementaria 3 (SSSE3), que deberían estar disponibles en cualquier procesador x86 moderno.

Además, Hyperscan puede hacer uso de:

- Extensiones Intel Streaming SIMD 4.2 (SSE4.2)

- La instrucción POPCNT

- Instrucciones de manipulación de bits (BMI, BMI2)

- Extensiones vectoriales avanzadas Intel 2 (Intel AVX2)

Software

Como biblioteca de software, Hyperscan no impone ningún requisito de software de tiempo de ejecución particular; sin embargo, para crear la biblioteca Hyperscan necesitamos un compilador moderno de C y C++; en particular, Hyperscan requiere compatibilidad con los compiladores C99 y C++11. Los compiladores soportados son:

- GCC, v4.8.1 o superior

- Clang, v3.4 o superior (con libstdc++ o libc++)

- Compilador Intel C++ v15 o superior

- Herramientas de compilación de Visual C++ 2017

Ejemplos de sistemas operativos en los que se sabe que funciona Hyperscan incluyen:

Linux:

- Ubuntu 14.04 LTS o más reciente

- RedHat/CentOS 7 o más reciente

Como se instala

La instalación de Hyperscan puede variar dependiendo del sistema operativo y las herramientas disponibles, pero generalmente sigue estos pasos:

1 Descarga del código fuente: Puedes obtener el código fuente de Hyperscan desde su repositorio en GitHub o desde el sitio web oficial.

https://github.com/intel/hyperscan

2 Requisitos previos: Hyperscan tiene dependencias de desarrollo que deben instalarse en tu sistema, como el compilador de C/C++, las herramientas de desarrollo y posiblemente algunas bibliotecas adicionales necesarias para la compilación.

3 Compilación: Después de descargar el código fuente y asegurarte de tener todas las dependencias necesarias, puedes compilar Hyperscan ejecutando los comandos de compilación proporcionados en la documentación o en el archivo README del repositorio.

1. Clone Hyperscan

```
cd <where-you-want-hyperscan-source>
git clone git://github.com/intel/hyperscan
```

2. Configure Hyperscan

Ensure that you have the correct dependencies present, and then:

```
cd <where-you-want-to-build-hyperscan>
mkdir <build-dir>
cd <build-dir>
cmake [-G <generator>] [options] <hyperscan-source-path>
```

4 Instalación: Una vez que la compilación se haya completado con éxito, puedes instalar Hyperscan ejecutando los comandos de instalación proporcionados. Esto copiará los archivos binarios y las bibliotecas necesarias en las ubicaciones adecuadas de tu sistema para que puedan ser utilizados por otras aplicaciones.

3. Build Hyperscan

Depending on the generator used:

- `cmake --build .` — will build everything
- `make -j<jobs>` — use makefiles in parallel
- `ninja` — use Ninja build
- `MsBuild.exe` — use Visual Studio MsBuild
- etc.

4. Check Hyperscan

Run the Hyperscan unit tests:

```
bin/unit-hyperscan
```

Integración de Hyperscan con snort

Hyperscan puede integrarse con Snort, que es un popular sistema de detección y prevención de intrusiones en red (IDS/IPS). La integración de Hyperscan con Snort permite mejorar el rendimiento de las reglas de detección, especialmente en entornos de alta velocidad donde se requiere un análisis rápido y eficiente del tráfico de red.

Descripcion general de la integración:

- Compilación de Snort con soporte de Hyperscan: Para habilitar la integración de Hyperscan con Snort, primero debes compilar Snort con soporte para Hyperscan. Esto implica configurar adecuadamente las opciones de compilación durante el proceso de configuración de Snort para que reconozca y utilice la biblioteca Hyperscan.

- Configuración de reglas de Snort para utilizar Hyperscan: Una vez que Snort está compilado con soporte para Hyperscan, puedes configurar reglas de detección en Snort para que utilicen

la funcionalidad de búsqueda de patrones de Hyperscan. Esto generalmente se hace mediante la especificación de las reglas de Snort en un formato que sea compatible con Hyperscan, lo que permite que Hyperscan realice búsquedas eficientes de los patrones especificados en el tráfico de red.

- Implementación y ejecución: Después de configurar las reglas de Snort para utilizar Hyperscan, puedes implementar y ejecutar Snort en tu red. Snort interceptará y analizará el tráfico de red en busca de posibles amenazas o actividades sospechosas utilizando las reglas especificadas, y Hyperscan acelerará este proceso al realizar búsquedas eficientes de patrones en el tráfico de red utilizando su tecnología optimizada.

- Monitoreo y respuesta a eventos: Snort generará alertas cuando detecte actividades sospechosas o coincidencias con las reglas especificadas. Estas alertas pueden ser monitoreadas en tiempo real por administradores de seguridad de red, y también se pueden configurar respuestas automáticas, como bloquear el tráfico malicioso o tomar otras medidas correctivas según sea necesario.

Conclusión

La integración de Hyperscan con Snort mejora el rendimiento y la eficiencia de la detección de amenazas en entornos de red al permitir búsquedas rápidas y eficientes de patrones utilizando la tecnología optimizada de Hyperscan. Esto es especialmente útil en entornos de alta velocidad donde se requiere un análisis rápido y preciso del tráfico de red para proteger contra amenazas en tiempo real.