Análisis de Logs

con Logsurfer

Mi Nombre <sergio.romero@soporte.rediris.es>

Descripción del proyecto

❑ Detección de actividades no permitidas

- SSH
  - ➢Accesos no permitidos.
  - ➢Ataques de diccionario.
- Apache
  - ➢ Recolección de scripts usados para comprometer el servidor.
  - ➢Tendencias y nuevos ataques.
- Generar estadísticas de los ataques sufridos.

Necesidades del servicio

- Detección de ataques hacia la comunidad.
  - ¿Cuantos ataque se producen al mes?
- Generar estadísticas de ataques sufridos.
  - Disponible para la comunidad.
  - Detección de nuevos patrones.
- Captura de scripts utilizados por los atacantes
  - Para su posterior análisis.

Inspección de logs

- Logsurfer
  - Busca patrones dentro de un fichero de texto.
- Scripts en Lenguaje Perl
  - Necesarios para automatizar el procesamiento posterior.

Logsurfer

- Desarrollado por DFN-CERT
  - Wolfgang Ley & Uwe Ellerman
  - http://www.cert.dfn.de/eng/logsurf/
  - http://sourceforge.net/projects/logsurfer/
- Análisis de Logs
  - Sobre ficheros ya creados.
  - Análisis en tiempo real del fichero.
- Motor de búsqueda utiliza la librería Regex
- Las búsquedas se editan en un fichero de configuración

Logsurfer

¿Por qué Logsurfer?

- Posibilidad de análisis en tiempo real.
- Posibilidad de creación de reglas dinámicas.
- Escrito en lenguaje C.
- Baja carga de máquina.
- Posibilidad de llamar a programas externos.
- Posibilidad de configurar mínimo de líneas necesaias para que se active la alarma.
- Edición de reglas de búsqueda mediante expresiones regulares.

Logsurfer

❑ Uso de Logsurfer

- Llamada al programa pasandole un Log
- Como Demonio (Analisis del log en tiempo real)
- Fichero de reglas de búsqueda.

Flujo de trabajo

- Detección de ataques recibidos.
  - Mediante Logsurfer
- Generar el Log y mandarlo a un buzón intermedio.
- Revisión del buzon intermedio
  - Descartar falsos positivos
- Envío de la denuncia.
  - Mediante el sistema RTIR
- Recolección y catalogación del binario (si lo hay)
  - Integración con proyecto BICHOS
- Generación de estadísticas

Objetivos/Fases de desarrollo

- Detección de actividades no permitidas.
  - Detección del ataque.
  - Denuncia al responsable de la IP orígen.
  - Integración de datos estadísticos en BBDD
- Recolección de código malicioso.
  - Recolección del binario.
  - Catalogación del binario en BBDD.
- Estadísticas.
- Generación a través de los datos recopilados.
- Generación de gráficas disponibles para la comunidad.

Estado actual del proyecto

- Detección de actividades maliciosas.
  - Completado el desarrollo, fase de pruebas.
- Generación de incidencias hacia el exterior.
  - Completado el desarrollo, fase de pruebas.
- Recolección de binarios
  - Fase de desarrollo.
- Estadísticas
  - Fase de desarrollo.

Futuro del proyecto

- Ampliación de sensores por parte de la comunidad.
  - Mayor cantidad de datos
- Extender el análisis de Logs a otros servicios.
  - Correo
  - FTP.