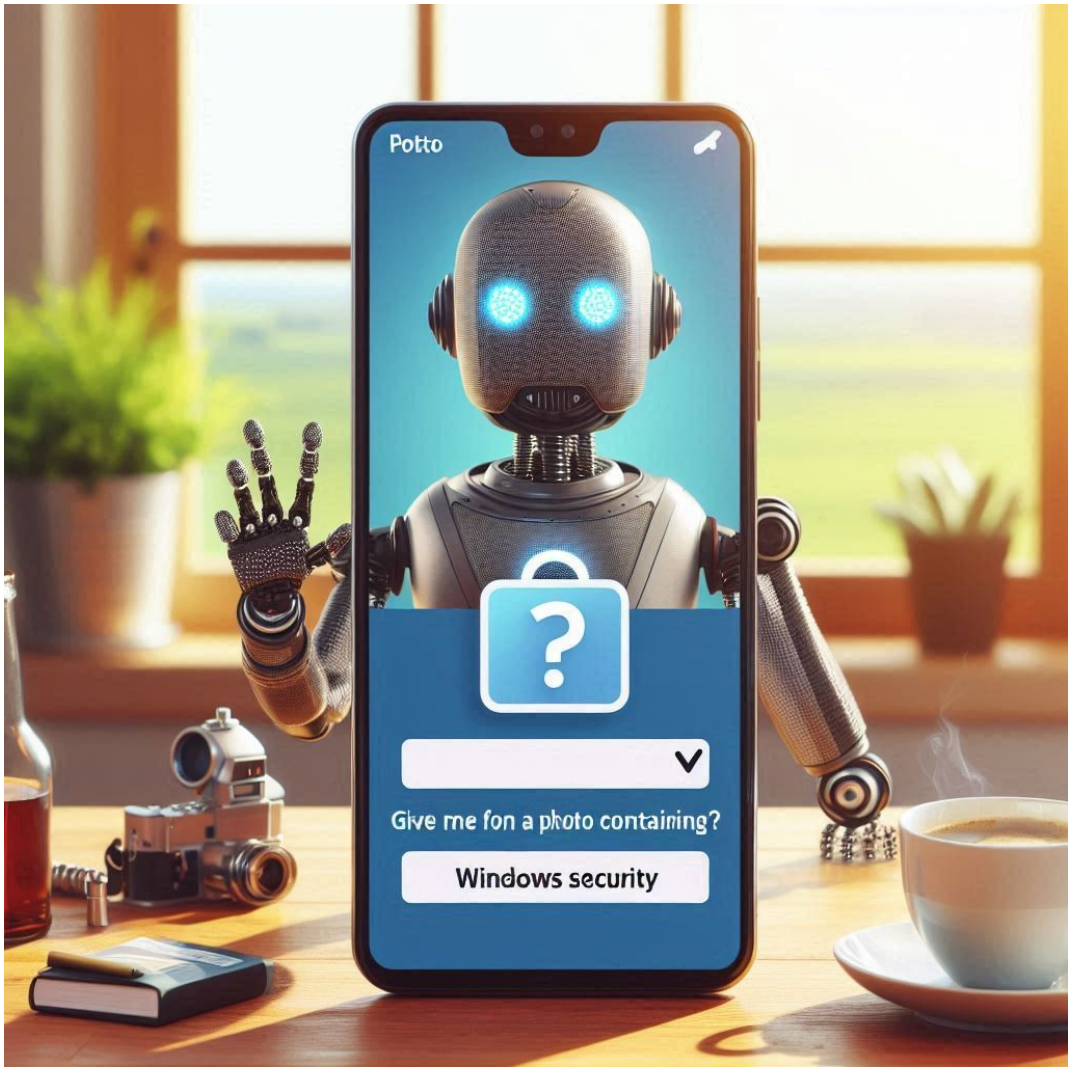
Analizador de inicios de sesión fallidos en Windows



Alumno: Martín Hernández Rodríguez
Curso: 1º ASIR

Introducción

En un entorno donde la seguridad informática es una preocupación constante, el proyecto "Analizador de inicios de sesión fallidos en Windows" surge como una herramienta valiosa para detectar y analizar intentos fallidos de acceso a sistemas Windows. Este proyecto, compuesto por un script Python y una aplicación web, ofrece una solución integral para mejorar la seguridad y la auditoría de los sistemas operativos Windows.

Descripción del proyecto

El proyecto se basa en un script Python que utiliza la biblioteca Flask para crear una aplicación web con las siguientes funcionalidades:

El proyecto "Analizador de inicios de sesión fallidos en Windows" se basa en un script Python que utiliza la biblioteca Flask para crear una aplicación web con las siguientes funcionalidades:

Análisis de logs:

- Permite analizar registros de eventos de Windows (.evtx) en busca de eventos de ID 4625, que indican intentos fallidos de inicio de sesión.
- Identifica y extrae información relevante de los eventos, como la fecha, hora, nombre de usuario, dirección IP y método de autenticación utilizado.
- Procesa grandes volúmenes de logs de forma eficiente.

Filtro de tiempo:

- Ofrece la posibilidad de filtrar los resultados por un rango de tiempo específico, permitiendo a los usuarios enfocarse en un periodo determinado.
- Define un rango de fechas personalizado o utiliza la configuración predeterminada (últimos 3 días).
- Facilita la identificación de patrones y tendencias en los intentos fallidos de inicio de sesión dentro de un marco temporal específico.

Notificación por Telegram:

- Envía un mensaje con los resultados del análisis a un bot de Telegram especificado.
- Resume la información clave sobre los intentos fallidos de inicio de sesión, incluyendo el número de intentos, el rango de fechas y los detalles de los eventos más relevantes.
- Facilita la comunicación y el seguimiento de los eventos por parte de los responsables de seguridad, incluso cuando no están frente a la aplicación web.

Interfaz web:

- Cuenta con una interfaz gráfica intuitiva que permite a los usuarios interactuar con la aplicación de forma sencilla.
- Proporciona un formulario para seleccionar los parámetros de análisis, incluyendo el rango de fechas y los archivos .evtx a procesar.
- Muestra los resultados del análisis de forma clara y organizada, utilizando tablas y gráficos para facilitar la comprensión.
- Permite a los usuarios descargar los resultados en formato CSV para un análisis posterior.

Tecnologías utilizadas

El desarrollo del proyecto se ha llevado a cabo utilizando las siguientes tecnologías:

- Python: Lenguaje de programación principal para el script y la lógica de análisis.
- Flask: Framework web para crear la aplicación web y gestionar las interacciones con los usuarios.
- Evtx: Biblioteca para leer y procesar archivos de registro de eventos de Windows (.evtx).

- Requests: Biblioteca para realizar solicitudes HTTP, como enviar mensajes a través de la API de Telegram.

- Telegram API: API para interactuar con bots de Telegram, permitiendo la comunicación y el envío de notificaciones.

Beneficios del proyecto

La implementación del "Analizador de inicios de sesión fallidos en Windows" ofrece una serie de beneficios para la seguridad y la auditoría de los sistemas:

- Mejora la seguridad:Permite identificar posibles intentos de intrusión en el sistema, alertando a los administradores y facilitando la toma de medidas preventivas.

- Facilita la auditoría: Simplifica la revisión de los eventos de inicio de sesión, proporcionando información detallada sobre los intentos fallidos de acceso.

- Automatiza el análisis: Automatiza el proceso de análisis de los logs, ahorrando tiempo y esfuerzo a los administradores de sistemas.

- Mejora la comunicación: Permite enviar notificaciones a través de Telegram, facilitando la comunicación y el seguimiento de los eventos por parte de los responsables de seguridad.

Posibles mejoras

El proyecto presenta un gran potencial para ser ampliado y mejorado en el futuro:

- Soporte para múltiples plataformas: Ampliar el soporte para otros sistemas operativos, como macOS o Linux, para abarcar un mayor rango de dispositivos y entornos.

- Análisis más detallado: Implementar un análisis más profundo de los eventos de inicio de sesión, incluyendo información sobre el usuario, la dirección IP, el método de autenticación utilizado y otros detalles relevantes.

- Visualización de datos: Implementar gráficos y tablas para visualizar los datos de forma más intuitiva, facilitando la comprensión de los patrones y tendencias en los intentos fallidos de inicio de sesión.

- Integración con herramientas SIEM: Integrar la aplicación con herramientas de gestión de eventos e información de seguridad (SIEM) para centralizar la gestión de logs y eventos de seguridad en un único panel de control.

- Aprendizaje automático: Implementar técnicas de aprendizaje automático para detectar patrones anormales en los eventos de inicio de sesión, mejorando la precisión de la detección de intrusiones.

Conclusión

El "Analizador de inicios de sesión fallidos en Windows" se presenta como una herramienta valiosa para mejorar la seguridad y la auditoría de los sistemas Windows. La aplicación web facilita el uso de la herramienta y permite a los usuarios interactuar con ella de forma sencilla. Las futuras mejoras ampliarán las capacidades de la aplicación y la convertirán en una herramienta aún más efectiva para la protección de los sistemas informáticos.

Recursos adicionales

Documentación de la biblioteca Evtx
Documentación de Flask
Documentación de la API de Telegram
Guía de seguridad para Windows Server
Mejores prácticas para la gestión de registros de seguridad