**Manual del Usuario del Hostbased Intrution Prevention System (HIPS)**

**1. Introducción**

Bienvenido al Manual del Usuario del Sistema de Prevención de Intrusiones en el Hogar (HIPS). Esta guía proporciona instrucciones paso a paso para la instalación, configuración y uso del HIPS con el fin de mejorar la seguridad de tu red y sistema en casa.

Para acceder al código ir al link [FilippiCR/hips: host based intrution prevention system (github.com)](https://github.com/FilippiCR/hips)

**2. Requisitos del Sistema**

Antes de proceder con la instalación, asegúrate de que tu sistema cumple con los siguientes requisitos:

Sistema Operativo: Basado en Linux (Ubuntu, Debian, etc.)

Python 3.x

Servidor de Base de Datos PostgreSQL

**3. Instalación**

Sigue estos pasos para instalar el Hostbased intrution prevention system (HIPS):

Abre una terminal en tu sistema Linux.

Clona el repositorio del HIPS desde GitHub: git clone https://github.com/FilippiCR/hips.git

Dirígete al directorio del HIPS: cd hips

Instala los paquetes de Python necesarios: pip install psycopg2 python-iptables

**4. Configuración de la Base de Datos**

Para configurar la base de datos del HIPS, sigue estos pasos:

Instala PostgreSQL en tu sistema si aún no lo has hecho: sudo apt-get install postgresql

Inicia sesión como el superusuario de PostgreSQL: sudo -u postgres psql

Crea una nueva base de datos y usuario para el HIPS:

CREATE DATABASE hips\_database;

CREATE USER hips\_user WITH PASSWORD 'tu\_contraseña\_de\_base\_de\_datos';

ALTER ROLE hips\_user SET client\_encoding TO 'utf8';

ALTER ROLE hips\_user SET default\_transaction\_isolation TO 'read committed';

ALTER ROLE hips\_user SET timezone TO 'UTC';

GRANT ALL PRIVILEGES ON DATABASE hips\_database TO hips\_user;

**5. Configuración de Variables de Entorno**

Por razones de seguridad, se recomienda almacenar la contraseña de la base de datos como una variable de entorno. Sigue estos pasos para configurar las variables de entorno:

Abre la terminal. Edita tu archivo de configuración de la terminal (~/.bashrc o ~/.zshrc):

vim ~/.bashrc

vim ~/.zshrc

Agrega las siguientes líneas al final del archivo:

export DB\_PASSWORD=tu\_contraseña\_de\_base\_de\_datos

Guarda el archivo y sal.

Recarga la configuración de la terminal: source ~/.bashrc

**6. Configuración y Uso**

Para configurar y utilizar el HIPS, sigue estos pasos:

Configura los ajustes deseados, como las rutas de los archivos de registro, intervalos de revisión y archivos supervisados.

**Configuración del Sistema de Logeo**

LOGS\_DIR = '/var/log/hips'

ALARM\_LOG\_FILE = os.path.join(LOGS\_DIR, 'alarmas.log')

PREVENTION\_LOG\_FILE = os.path.join(LOGS\_DIR, 'prevencion.log')

USER\_LOG\_FILE = os.path.join(LOGS\_DIR, 'usuarios.log')

CHECK\_INTERVAL = 180

**LOGS\_DIR:** Directorio donde se almacenarán los archivos de log del HIPS.

**ALARM\_LOG\_FILE:** Ruta completa al archivo de log de alarmas.

**PREVENTION\_LOG\_FILE:** Ruta completa al archivo de log de prevención.

**USER\_LOG\_FILE**: Ruta completa al archivo de log de usuarios.

**CHECK\_INTERVAL:** Intervalo de tiempo (en segundos) entre las verificaciones del HIPS.

**Configuración de la Base de Datos**

DB\_NAME = "hips\_database"

DB\_USER = "hips\_user"

DB\_PASSWORD = os.environ.get("DB\_PASSWORD")

DB\_HOST = "localhost"

DB\_PORT = "5432"

**DB\_NAME:** Nombre de la base de datos utilizada por el HIPS.

**DB\_USER:** Nombre de usuario para acceder a la base de datos.

**DB\_PASSWORD:** Contraseña de la base de datos obtenida de la variable de entorno.

**DB\_HOST:** Dirección del host de la base de datos (en este caso, local).

**DB\_PORT:** Puerto de la base de datos PostgreSQL.

**Lista de Herramientas de Captura de Paquetes**

packet\_capture\_tools = [

{"name": "tcpdump", "uninstall\_cmd": "apt-get remove tcpdump -y"},

{"name": "wireshark", "uninstall\_cmd": "apt-get remove wireshark -y"},

{"name": "tshark", "uninstall\_cmd": "apt-get remove tshark -y"},

{"name": "ethereal", "uninstall\_cmd": "apt-get remove ethereal -y"},

]

**packet\_capture\_tools:** Lista de herramientas de captura de paquetes que el HIPS verificará. Cada herramienta tiene un nombre y un comando para desinstalarla en caso de detección.

**Definición de Binarios del Sistema**

system\_binaries = [

"/bin/ls",

"/bin/ps",

"/usr/bin/gcc",

"usr/bin/passwd",

"/bin/ping",

"/bin/su",

"/sbin/ifconfig"

"/usr/bin/sudo"

"/bin/mount"

"/sbin/ip"

# Agregar más binarios según sea necesario

]

**system\_binaries:** Lista de rutas a binarios del sistema que el HIPS supervisará en busca de modificaciones.

**Definición de Archivos a Monitorear**

python

Copy code

files\_to\_monitor = [

"/etc/shadow",

"/etc/passwd"

# Agregar más archivos según sea necesario

]

**files\_to\_monitor:** Lista de rutas a archivos que el HIPS supervisará en busca de modificaciones.

**Lista de Direcciones de Correo Electrónico a Monitorear**

monitored\_email\_addresses = ["sender@example.com", "another\_sender@example.com"]

**monitored\_email\_addresses:** Lista de direcciones de correo electrónico que el HIPS supervisará para detectar envíos masivos de correos.

**Ejecuta el script del HIPS:**

python hips.py

El HIPS ahora supervisará los binarios del sistema, archivos y otras actividades en busca de posibles amenazas de seguridad.

7. Solución de Problemas

Si encuentras algún problema durante la instalación o el uso del HIPS, consulta los siguientes pasos de solución de problemas:

Revisa los registros: El HIPS genera registros en el directorio /var/log/hips. Revisa los registros en busca de mensajes de error e indicios sobre el problema.

Verifica las dependencias: Asegúrate de que todas las dependencias necesarias estén instaladas y actualizadas.

Verifica la conexión a la base de datos: Asegúrate de que los detalles de conexión a la base de datos sean correctos.