**Ingeniería de Seguridad del Software**

**Práctica de Laboratorio No 3:**

**Tema: Análisis de un keylogger en Kali Linux y desarrollo de un keylogger básico con Python.**

**Objetivos de aprendizaje:**

* Los estudiantes comprendan el funcionamiento de un keylogger y su implementación en un entorno controlado utilizando Kali Linux.
* Los estudiantes aprenderán a configurar y ejecutar un keylogger, observarán su funcionamiento, y analizarán su impacto en la seguridad.
* Los estudiantes se abordarán aspectos éticos relacionados con el uso de este tipo de herramientas.

**Topología:**

1. **Kali Linux** (máquina atacante).
2. **Windows o Linux** (máquina víctima, puede ser una máquina virtual).
3. **Keylogger libre: "Logkeys"** (preinstalado en Kali Linux o puede instalarse fácilmente).
   * [Logkeys](https://github.com/kernc/logkeys): es un keylogger para Linux que permite registrar las teclas pulsadas por el usuario.
4. **Wireshark o iptraf** (para análisis de red, opcional).

**Desarrollo:**

**Instalación y Configuración del Keylogger**

1. **Instalar Logkeys en Kali Linux**:
   * En Kali Linux, abre la terminal y verifica si **Logkeys** está instalado. Si no está instalado, utiliza el siguiente comando para instalarlo:

$ sudo apt-get install logkeys

1. **Configurar Logkeys**:
   * En Kali Linux, ejecuta **Logkeys** para iniciar la captura de teclas:

sudo logkeys -s /home/usuario/logfile.txt

* + Esto comenzará a grabar las teclas pulsadas en un archivo de texto en el directorio especificado (logfile.txt).

1. **Verificar la ejecución del Keylogger**:
   * En la máquina víctima, abre un editor de texto o una terminal y empieza a escribir. Los caracteres tecleados deben ser capturados por el keylogger en Kali Linux.

**Evaluación de Resultados**

1. **Monitoreo de la captura de teclas**:
   * En la máquina víctima, los estudiantes deben escribir en aplicaciones como un navegador web, un procesador de texto o la terminal para generar entradas de teclado.
2. **Ver los resultados**:
   * En Kali Linux, abre el archivo de texto (logfile.txt) donde las teclas se están registrando:

cat /home/usuario/logfile.txt

* + Los estudiantes deben ver todas las teclas que se han presionado en la máquina víctima.

**Discusión: Reflexión y Consideraciones Éticas**

1. **Discusión en grupo**:
   * Después de completar la práctica, los estudiantes deben discutir en sus grupos sobre el funcionamiento del keylogger, los riesgos que conlleva su uso y cómo puede afectar la seguridad de una red.
2. **Consideraciones éticas**:
   * Los estudiantes deben reflexionar sobre las implicaciones éticas del uso de herramientas como keyloggers.
   * **Pregunta para debate**: ¿Es ético usar un keylogger sin el consentimiento del usuario? ¿Qué responsabilidades tienen los ingenieros en seguridad para prevenir este tipo de ataques? ¿Existe alguna ley o reglamento que juzgue y sancione esto?

**Trabajo de investigación.**

Desarrolle un keylogger en Python, y realice las pruebas respectivas de detección. Luego implemente un programa en Python o en C ANSI para detectar, controlar y mitigar el ataque basado en keylogger.

**Conclusión de la práctica:**

Al final de esta práctica, los estudiantes habrán adquirido experiencia práctica con el uso de un keylogger en un entorno controlado, comprendiendo tanto su funcionamiento como las consecuencias de su uso en términos de seguridad informática. Sí mismo aprenderá a programar un kelygger en Python a detectarlo y a mitigarlo.   
Se enfatiza la importancia de la ética en el campo de la ingeniería y la seguridad, especialmente cuando se trata de herramientas que pueden invadir la privacidad de las personas.

**Referencias bibliográficas**