EPP (Enpoint Protection Platform)

Es un método de ciberseguridad que busca analizar paquetes con posible malware, endpoints con posibles vulnerabilidades y amenazas en la red, además de intercambiar datos con otros sistemas de seguridad. Tiene la ventaja de poder hacerse de una manera centralizada en la que podamos monitorear cada endpoint desde una sola consolad de comandos, en lugar de revisar cada equipo físicamente. Un EPP se puede empalmar con otros métodos de ciberseguridad como un DLP para impedir la pérdida de datos o un EDR para el escaneo constante de los archivos y endpoints en nuestra máquina.

Funciones Básicas:

1. Escaneo de archivos
2. Monitoreo de Procesos sospechosos
3. Protección en tiempo real o bajo demanda

Tecnologías:

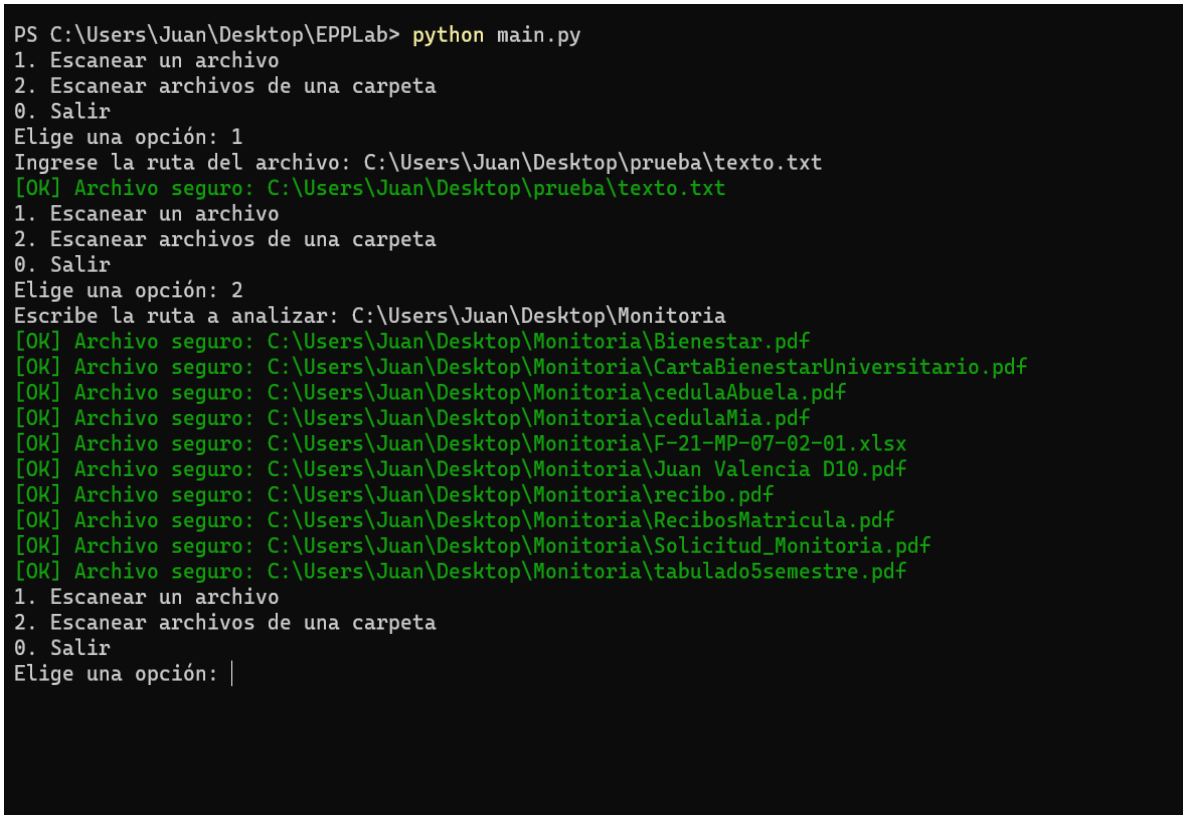
1. Python
2. YARA
3. Syscalls

Para este proyecto se enfocará en desarrollar un Endpoint bajo demanda, es decir se utilizará un menú para pedirle al usuario que directorio quiere escanear o que archivo en específico quiere pasarle al programa. Se hará manejo de las reglas YARA para un análisis estático de los archivos. En las reglas se tiene en cuenta funciones como las llamadas a la syscall de Windows con eventos que puedan registrar teclas esto para detectar keyloggers, se tiene en cuenta también código de ensamblador para el caso de las shellcodes, se revisa también las conexiones a los servicios ftp y http.

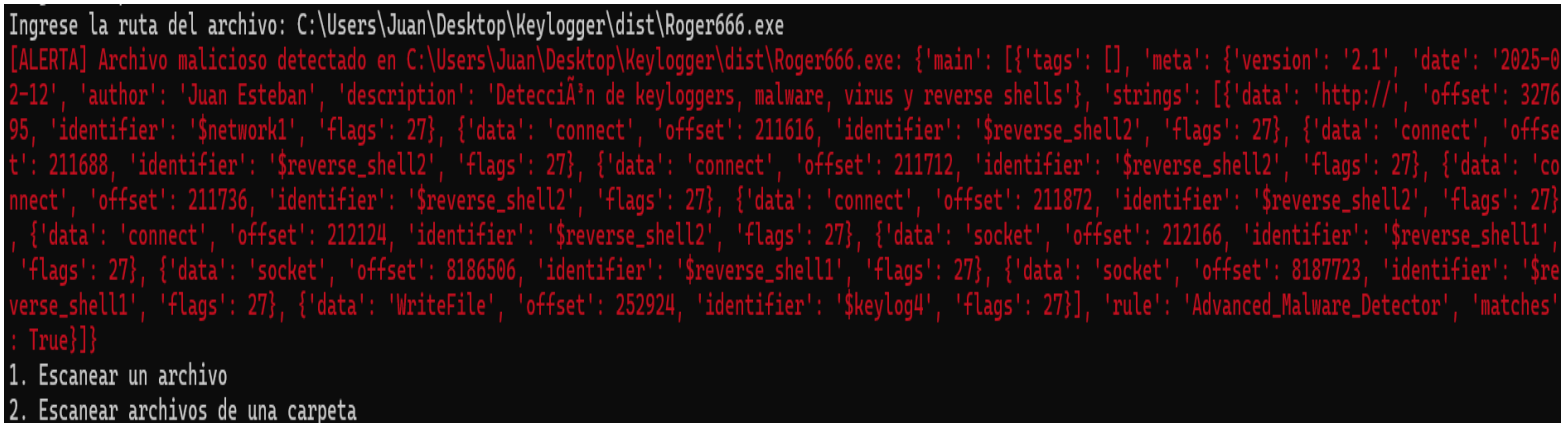
Este es un avance del EPP.

Menú del programa.

Prueba del programa con archivos individuales y archivos de un directorio.



Análisis de un keylogger.



Como se puede ver el EPP cumple con sus funcionalidades básicas la de detectar malware en un ejecutable y pasar los archivos limpios como libres del malware sin embargo esto no lo hace exento de falsos positivos o de malas gestiones a otros archivos, por ejemplo el ejecutable del Rogger666 el cual es un keylogger lo pasa como malware pero su código Python no lo ve como un peligro.

Este EPP sigue en desarrollo sin embargo es un buen ejemplo de como manejar las reglas yara a nuestro favor y como podemos automatizar procesos utilizando Python.