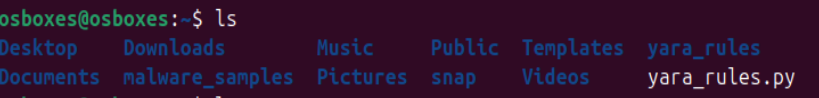
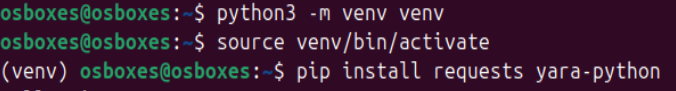
A screenshot of a computer

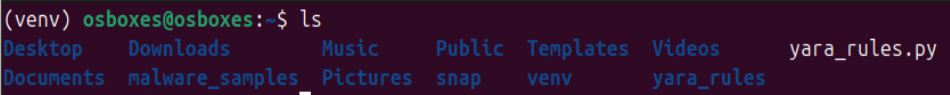
AI-generated content may be incorrect.











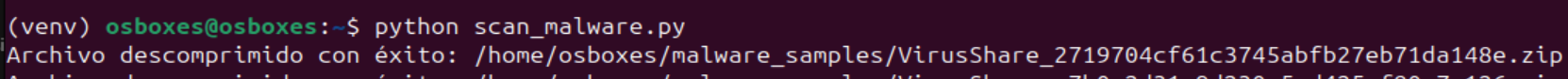
Para descargar las reglas Yara de los repositorios de GitHub de Cape y FeversingLabs utilice el programa yara\_rules.pg

A computer screen with white text

AI-generated content may be incorrect.

A computer screen shot of a program

AI-generated content may be incorrect.





A screenshot of a computer program

AI-generated content may be incorrect.

A computer screen shot of a computer code

AI-generated content may be incorrect.

Descarge las reglas Yara del ***Github-ThreatHunting -signature\_keyword*** como se muestra a continuación:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

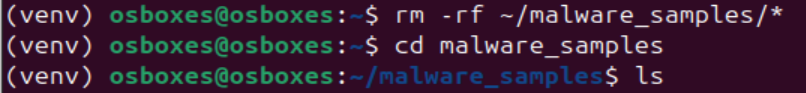
AI-generated content may be incorrect.

Descargue todas las reglas Yara del subdirectorio **signature\_keyword** en el subdirectorio que aparece a continuación y ahora me queda colocarlas todas en un subdirectorio que llamare **signature\_keyword** en el subdirectorio **yara\_rules** original.

A computer screen with text

AI-generated content may be incorrect.

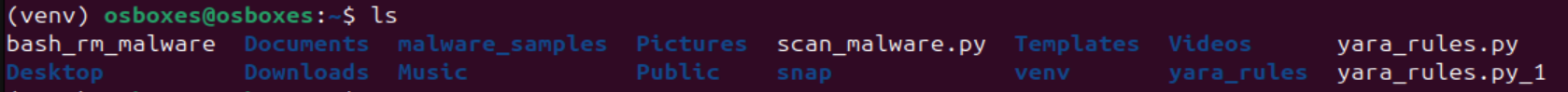
Si en la ejecución de las pruebas del programa necesito eliminar el contenido del subdirectorio malware\_samples por alguna razón como que el programa repita los .exe cada vez que se ejecute el siguiente comando lo hace:



Copio el Malware/Ransomware .exe Windows, que está en /Home/Downloads/ al subdirectorio de malware\_samples:

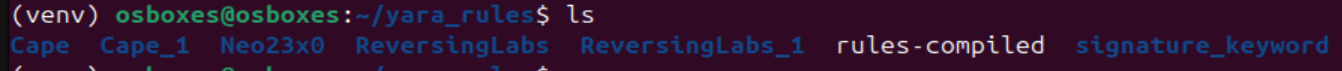
El siguiente screenshot muestra el bash para compilar las reglas yara manualmente de tres repositorios de GitHub: Cape, ReversingLabs y el subdirectorio signature\_keyword de ThreatHunts. Pero antes tuve que cambiar los permisos porque no me dejaba crear el archivo **rules\_compiled**.



 A screenshot of a computer

AI-generated content may be incorrect.

Ahí aparece el archivo rules\_compiled.



A computer screen with red and white text

AI-generated content may be incorrect.

El programa Python siguiente descompacta de .zip a .exe:

