Herramientas utilizadas en seguridad informática escritas en Python

* Volatility: Volatility es un marco forense de memoria de código abierto para la respuesta a incidentes y el análisis de malware. Está escrito en Python y es compatible con Microsoft Windows, Mac OS X y Linux
* SET (Social engineering toolkit): Es una completísima suite dedicada a la ingeniería social, que nos permite automatizar tareas que van desde el de envío de sms falsos, con los que podemos suplantar el número telefónico que envía el mensaje, a clonar cualquier página web y poner en marcha un servidor para hacer phishing en cuestión de segundos.

c

https://github.com/volatilityfoundation/volatility

* SQLmap: sqlmap es una herramienta de prueba de penetración de código abierto que automatiza el proceso de detección y explotación de fallas de inyección SQL y la toma de control de los servidores de bases de datos.

https://github.com/sqlmapproject/sqlmap

* Canvas: Canvas es una herramienta comercial de explotación de vulnerabilidades de ImmunitySec de Dave Aitel. Incluye más de 370 exploits y es menos costoso que Core Impact o las versiones comerciales de Metasploit. Viene con código fuente completo y, en ocasiones, incluso incluye exploits de día cero.

c

* SPARTA: es una aplicación con la cual nos simplifica las pruebas de penetración en una determinada infraestructura de red y nos permite realizar diversas pruebas de penetración en la fase de escaneo y enumeración.

https://github.com/SECFORCE/sparta

* Pydbg: Es un debugger de ring que nos permite ejecutar un programa y estudiar todas las acciones que realiza en el sistema, pudiendo definir los breakpoints y hooks.

https://github.com/OpenRCE/pydbg

* Pompem: Es una herramienta de código abierto que está diseñada para automatizar la búsqueda de vulnerabilidades en las principales bases de datos.

https://github.com/rfunix/Pompem

* Blindelephant: Es una herramienta basada en python que se utiliza para realizar fingerprinting en aplicaciones web.

https://github.com/lokifer/BlindElephant

* Rekall: es una colección de herramientas completamente abierta para la extracción y análisis de sistemas informáticos de artefactos digitales.

https://github.com/google/rekall

* Exefilter: ExeFilter es una herramienta y un marco de código abierto para filtrar formatos de archivo en correos electrónicos, páginas web o archivos. Detecta muchos formatos de archivo comunes y puede eliminar contenido activo (scripts, macros, etc.) según la configuración.<https://github.com/decalage2/exefilter>.
* Impacket, Herramienta para trabajar con paquetes y payloads de multiples protocolos, especialmente SMB. [GitHub - SecureAuthCorp/impacket: Impacket is a collection of Python classes for working with network protocols.](https://github.com/SecureAuthCorp/impacket)
* NoSQLMap, port de SQLMap pero adaptado a sistemas DBMS de NoSQL [GitHub - codingo/NoSQLMap: Automated NoSQL database enumeration and web application exploitation tool.](https://github.com/codingo/NoSQLMap)
* OneLiner Herramienta con un set de templates utiles para escalacion de privilegios [GitHub - D4Vinci/One-Lin3r: Gives you one-liners that aids in penetration testing operations, privilege escalation and more](https://github.com/D4Vinci/One-Lin3r)