6. Python y PowerShell

Wednesday, November 4, 2020 8:05 AM

El proceso de búsqueda es el paso principal en las investigaciones digitales. Sin embargo, en las últimas décadas, la cantidad de datos a investigar, la variedad de los tipos de contenido y el tipo de información necesaria para conectar toda la evidencia a un incidente o, inclusive, a una actividad criminal, ha aumentado exponencialmente.

Debemos considerar que la evidencia digital no constituye un conjunto de datos estáticos, sino que esta constantemente cambiando, por lo que los tiempos en los que la examinamos y como la examinamos se vuelven factores cruciales.

Siendo Python y PowerShell dos herramientas poderosas en las actividades de seguridad informática, especialmente para temas de recolección de evidencia digital (muy útil en informática forense), se busca integrar actividades de adquisición de datos a través de PowerShell con la potencia de Python. Los métodos principales para hacer esto son:

- Método 1: Ejecutar los scripts o CmdLets de PowerShell y recolectar los datos posteriores al proceso utilizando Python.
- Método 2: Ejecutar los scripts o CmdLets de PowerShell y conectar los resultados a los scripts de Python que esperan por ellos.