

Utilidad de un Osquery para un Sistema

Autor: Wellington Andres Martinez

Unidad educativa: ESPOL





Resumen

Los Osquery son actualmente una herramienta muy útil y poderosa para un sistema operativo que intenta dar un enfoque diferente al enfoque de los sistemas operativos de bajo nivel, el cual afecta de forma positiva al tiempo de ejecución, el tiempo de carga de los módulos en el kernel, etc. La consola provista por el Osquery a la base de datos permite interactuar de forma diferente con los sistemas operativos del comportamiento que actualmente estos presentan. Todo esto es posible gracias a que el código permite un gran rendimiento a las aplicaciones.

Introducción

“Osquery es un framework diseñado para dar un enfoque diferente a los sistemas operativos de bajo nivel, exponiendo el enfoque utilizado en los sistemas operativos de alto nivel, el objetivo que se ha dado al mismo es enfatizar en un mejor rendimiento y velocidad en tiempo de ejecución del sistema operativo al que este fuere aplicado al proveer a este una interfaz que permita interactuar con el mismo”.

“Esta interfaz está provista de diversas aplicaciones que afectan al sistema de diversas formas.”

-  Manipulación del código base modular
-  Implementación de código abierto
-  Provee del uso de una multiplataforma
-  Uso de paquetes nativos y documentación extensa

“Son algunas de las aplicaciones que el framework Osquery provee al sistema operativo en el que se encuentra operando”.

Contenido

“Muchas veces hemos interactuado con la interfaz que nos proporciona facebook para muchas de sus aplicaciones como”.

1. Añadir amigos

2. Eliminar amigos
3. Búsqueda de amigos

“Sin embargo lo que no conocemos es que dicha interfaz es provista por un framework en particular, este es conocido como Oequery y su principal objetivo es”:

“Proveer a un sistema operativo de bajo nivel un funcionamiento similar al de uno de alto nivel, con el objetivo de mejorar el rendimiento, tiempo de ejecución entre otros factores de dicho sistema operativo”.

Conclusiones

“Osquery es una herramienta muy útil que provee muchas facilidades al sistema operativo en el que está trabajando, sin embargo no es una herramienta muy común ni muy utilizada en la actualidad dado que muy pocas plataformas conocen de las ventajas y usos del mismo, lo que nos lleva a hacernos la pregunta: ¿Es correcto el uso de la framework Osquery a nivel general?, la respuesta puede depender del punto de vista de la empresa que esté interesada en el uso de este framework”.