

Los riesgos ligados al scripting

Observará rápidamente en qué se basa la fuerza del scripting, aunque también podrá ver su fragilidad. La facilidad con la que se pueden hacer las cosas, haciendo sencillamente un clic en un script, o ejecutándolo desde una ventana de comando, puede crearle una situación embarazosa si no tiene cuidado.

Supongamos un script de logon que desde el inicio de la sesión la bloquea inmediatamente. Esto puede ser divertido entre amigos, pero en una empresa, dudamos que esté muy bien visto. Aún más grave, un script procedente de una persona con malas intenciones o muy poco experimentada en PowerShell (en este caso, le recomendamos comprarle un ejemplar de este libro...) puede perfectamente bloquearle las cuentas de usuario en Active Directory, formatearle un disco, hacer que tenga que reiniciar sin cesar. En fin, lo ha entendido, un script puede hacerlo todo. Porque, aunque actualmente se hacen llegar alertas al usuario para prevenir de la ejecución de un script, no son capaces de determinar de antemano si un script es perjudicial para el buen funcionamiento del sistema.

Los riesgos relacionados con el scripting se reducen a una cuestión de compromiso: o bien decide impedir cualquier ejecución de scripts, y por lo tanto asume que deberá pasarse la vida haciendo y rehaciendo tareas básicas que suelen ser ingratas, o bien decide abrir su sistema al scripting, tomando las precauciones adecuadas.

Pero no se desmoralice ya que incluso si la ejecución de los scripts le expone a algunos problemas de seguridad, PowerShell está dotado de nuevos conceptos que facilitan considerablemente este aspecto del scripting.