¿Qué es eso de pentesting Cloud y las diferencias al pentesting tradicional?

La principal diferencia cuando vamos a empezar a realizar una prueba de seguridad o pentesting cloud, es informar a la empresa que brinda el servicio de la nube, Que significa esto, que si yo voy a realizar una prueba sobre una infraestructura montada sobre amazon, azure o google, lo primero que voy a tener que hacer es informar la actividad que voy realizar, ya que sino de otra manera la empresa nos puede bloquear, ya que se realizaría una actividad que no se encontraba dentro del encuadre contractual. Esta instancia es una gran diferencia con el pentest tradicional, donde a pesar de contar con la autorización de la empresa debemos buscar la de quien presta el servicio de infraestructura en la nube.

La otra gran diferencia que podemos encontrar es las herramientas que vamos a utilizar. Donde usar un nmap, un nessus, ¿Por qué?, simple, usar estas herramientas en este contexto no va a tener mucho sentido, ya que vamos a estar invirtiendo tiempo energía y recursos en algo que con suerte solo nos va a devolver como resultado un puerto 80 abierto que nos deja Amazon. Tirar una detección de owasp contra un servidor cloud, no tiene mucho sentido ya que nos va a devolver aws protected.

Esto ha cambiado el tiempo y la forma de iniciar este análisis.

Para quienes inician en pentesting pueden intentar llevar herramientas onpremis al mundo cloud y con lo explicado uno se da cuenta que no tiene mucho sentido.