**¿Qué diferencia hay entre un Pentest tradicional vs Cloud?**

Quizás los pasos son los mismos tratar de relevar información hacer inteligencia sobre el objetivo porque saben bien geniales. El primer paso para cualquier pentes. Después una vez obtenida la información tratar de listar los servicios que están etc. o sea los pasos son los mismos lo que cambia radicalmente la forma de llevarla adelante y ante todo hay que agregar un paso cero que era el que yo dije al principio que es tratar de comprender cuáles son las políticas de análisis que me deja hacer el proveedor de cloud. ué significa esto. Yo mañana contra aws por decir algo que es el tema que tienen más del 50 por ciento del mercado. Contrato Amazon y no me leo la política el documento que te dan 400 hojas que tenés que firmar, lo cual firmas por defecto que literalmente tienen 400 hojas en donde ellos te dicen si vos querés probar una aplicación tuya pero que esté instalada sobre mi infraestructura. Primero me vas a tener que pedir permiso y yo te voy a tener que conceder ese permiso. En general no tienen problema en dártelo lo que no les gusta es que no les avises. Entonces qué pasa. Yo mañana por ejemplo un tirar un nmap y lo empiezo a tirar y me va a llegar una alerta diciéndome que detectaron un escaneo desde mi dirección IP y que directamente el servicio, de hecho tengo clientes que ya ha pasado en donde directamente el servicio deja de concederce y te cierran el acceso tan sencillo como eso es como que te causa una auto denegación de servicio simplemente porque quieres probar si tu servicio funcionaba. Ese es el primer paso. El segundo cambia un poco, el tema de el plan de testing cambia a cabo va a tener aplicaciones que voy a poder probar en el caso de que tengas un software instalado independientemente de que si está sobre una aplicación sobre una plataforma mía o sobre una plataforma del proveedor voy a tener que probar acceso a los datos y todo lo que tenga que ver con el acceso a la red específicamente no es lo mismo probar una red de un proveedor en cloud que de una de un proveedor de un onpremis. Por qué?. Porque en general todo lo que es el ambiente Cloud yo voy a tener por ejemplo 10 empresas. Alojadas en el mismo servidor virtual del proveedor. Yo podría probar una cosa que no voy a poder probar en un entorno tradicional, es decir a ver si dentro del entorno “a” estoy parado en el entorno “a” sea con permisos o porque accedí de alguna manera, no será posible entonces también acceder al entorno en donde el entorno es de mi competencia por ejemplo. Entonces eso hay en una infraestructura tradicional no se prueba porque no existe ese modelo. Sería como que yo tengo dos máquinas virtuales me colo en la primera y ahí quiero saltar a la segunda eso sería lo más parecido. Eso cambia radicalmente de una estructura infraestructura de cloud versus una estructura típica de tradicional de una empresa.

También cambia el modelo de análisis de red y de análisis de virtualización. Por qué?. Porque si yo quiero probar. Las máquinas virtuales en un entorno onpremis va a depender de cómo las configure yo y qué tanto sepa de mi entorno de virtualización y de cuanto qué tan bueno sea el administrador. En cambio en una infraestructura de cloud voy a tener seguramente aplicada por defecto como dije antes las mejores prácticas. Por lo tanto vulnera intentar vulnerar un SKI versión 6 que no tiene parches no tiene sentido. Por qué. Porque por defecto en un entorno cloud yo sé que voy a tener la última versión de la aplicación de virtualización y voy a tener los últimos parches de esa aplicación.

Y por otro por otro lado algo fundamental que cambia mucho radicalmente el entorno cloud es el tema de la administración de usuario. No sé si para los que tengan experiencia por ejemplo administrando Amazon o lo que tengan experiencia azure. Hay cientos de perfiles literalmente cientos de tipos de perfiles que ya vienen preconfigurado y lo único que yo tengo que hacer es administrar bien los usuarios los grupos de usuarios y los grupos de seguridad que con un nombre también relativamente nuevo que aparecen en cloud. Por lo tanto eso en realidad es tarea de configuración que si eso yo lo quisiera hacer en un entorno premis lo tendría que configurar uno por uno para cada uno de los perfiles y cada uno de los permisos que quiero dar. Me a tocado probar una vulnerabilidad en una empresa sobre Docker la cual fue critica, donde la misma demoro 24 horas en implementar ya que el parche de la misma implicaba cambios críticos donde podían significar que deje de funcionar. Esto se vio en empresas de primera línea como azure o aws, Entonces tuvieron que evaluar todas las posibilidades antes de implementar el parche. Estamos hablando como máximo 24 horas. Si yo eso lo tendría que hacer en una infraestructura mía capaz que estoy un mes analizándolo y por miedo capaz que después no lo instalo por qué digo si ya está funcionando lo viejo así.

La clásica teoría que tenemos todos. Sí todo esta andando bien no lo toques porque funcion. Pero digamos no es demasiado normal encontrar vulnerabilidades de falta de parches en un entorno cloud. La verdad es que no es para nada normal. Cosa que sí es normal en un entorno tradicional onpremis. Totalmente normal.

Charles fue el alemán que en ese caso Amazon aplicó inmediatamente el parche recomendado por Intel para Spectre y lo que observó inmediatamente 24 horas después fue una caída significativa en el rendimiento de la CPU. Estamos viendo caída significativa del 2 3 por ciento lo cual para un tamaño de infraestructura de Amazon eran millones de dólares en pérdidas de plataformas y millones de dólares en pérdida de conectividad y usuarios que se quejaban básicamente que eso es lo que hizo fue que mejoraran de hecho escribieron un paper al respecto y todo en donde dijeron Bueno la vulnerabilidad para Spectre se soluciona así pero nosotros la solucionamos de esta manera para que no haya pérdida caída de performance en los procesadores que nosotros utilizamos en nuestro propio entorno. Eso es todo eso que estoy contando lo hicieron en menos de 48 horas para que sea una idea de cómo evoluciona rápido en el mercado de cloud y cómo responden rápido a este tipo de proveedores.