Problemas Encontrados

Sergio Rosello Morell

Durante la realización de la practica, se han encontrado varios problemas. Desde no poder configurar la comunicación entre las maquinas mediante el entorno NPC de Amaron Web Servicies, hasta no conseguir que se configuren correctamente debido a la falta de información sobre la red virtual en la que están alojados. A lo largo de este documento, se especificaran los problemas encontrados, ademas de como se han solucionado.

Gestión del entorno VPC

Al iniciar la configuración del entorno, sabia que para poder configurar un SOC Security Onion a nivel de producción, era necesaria la comunicación entre varias maquinas. Siendo estas el servidor y los sensores.

Para poder habilitar la comunicación entre estas maquinas, es necesario que residan todas en una misma red.

La dificultad de esta configuración ha sido revelada cuando he sabido de la necesidad de las maquinas sensor de tener dos interfaces de red. Estas interfaces se han tenido que configurar en la misma VPC y agregar a los sensores.

Obtención de la IP del servidor DNS

En la primera imagen descargada y configurada desde AWS, el script de configuración nos pregunta por la IP del servidor DNS. Al ser una red virtual auto generada por AWS, he tenido que buscar exactamente donde estaba el servidor DNS alojado.

Resulta que en cada VPC proporcionada por AWS, el servidor DNS esta en la IP base del grupo CIDR que gestiona la red virtual + dos direcciones IP. Es decir, la IP del servidor DNS existe en 172.31.0.2

Comunicación SSH entre servidor y sensores

Las maquinas de AWS por defecto, por seguridad no permiten el inicio de sesión por SSH mediante contraseñas, pero la herramienta de configuración de las maquinas necesita poder configurarlo para que se puedan comunicar en un primer momento. Por esto, he tenido que habilitar la autenticación por contraseña para posteriormente deshabilitaría de nuevo, una vez la configuración inicial había terminado.

Instalación de imagen errónea, proporcionada por AWS

Durante los primeros días de la instalación, se ha usado la siguiente imagen proporcionada por AWS

Figure 1: SO-AMI

El problema, entonces venia en que la herramienta de configuración no era tan avanzada. En el momento en el que acababa de configurar la maquina como manager y revisaba el estado de la misma, parecía que no funcionara nada.

Instalación imposible desde OVA

Al ver que este camino me era inviable, he decidido optar por descargar la imagen proporcionada por securityonion, instalarla en local, generar un .OVA para subir a AWS y poder generar la instancia EC2 a partir de la misma. El proceso de generado del archivo que necesita AWS para poder generar la instancia a partir de un OVA especifico ha ido bien, pero en el momento en el que tenia que subir la imagen a AWS, necesitaba un usuario con acceso programático a AWS. El problema aquí es que no se pueden crear usuarios con acceso programático a AWS desde nuestras cuentas. Esto me ha llevado a usar una maquina Ubuntu estándar de AWS y posteriormente descargar el repositorio de GitHub que proporciona Security Onion para poder configurarla como manager.

Instancia de Analista

Al acabar la configuración inicial, he querido dar un paso mas, para instalar la maquina del analista, que se conectara a "manager" para observar el estado de la red. Al descargar y ejecutar el script que proporciona securityonion, este mismo notifica que la única distribución de GNU/Linux que soporta es CentOS 7.

Esta distribución existe como AMI, pero esta disponible en el marketplace, al que no podemos acceder con los permisos de nuestro usuario.

Posteriormente, se ha editado el script para que no revise el tipo de sistema en el que esta corriendo y se ha modificado la forma de descargar los paquetes, de yum a apt.

Finalmente, se ha decidido añadir una regla al VPC de AWS para que acepte la dirección IP desde la que me conecto y se ha añadido el `hostname` del servidor a mi archivo local `/etc/hosts` para poder acceder a el desde `https://manager` ## Conclusión

Como en todo proyecto, al menos en mi experiencia, son mayores las ganas de configurar y trastear que las de seguir los manuales. En esta ocasión, este impulso me ha llevado a aprender mas sobre el entorno AWS en el que estaba haciendo la practica, por tanto, no puedo decir que haya perdido el tiempo en absoluto.