Práctica 2. Análisis forense en la nube.

Extracción de evidencias de VM on-premise/IaaS

Una de las situaciones a las que nos podemos enfrentar como futuros profesionales de las periciales forenses es enfrentarnos a máquinas virtuales, bien en instalaciones propias (nuestras o del cliente) o de terceros.

En instalaciones propias tenemos más posibilidades de actuación. Podemos actuar desde dentro de la propia máquina virtual o desde el virtualizador. La primera situación con dista demasiado de las que ya hemos trabajado en clase: podemos usar dumpit o software similar para realizar un volcado de memoria, ejecutar un script de extracción de artefactos y también realizar un clonado de disco duro u obtener una imagen lógica en el peor de los casos.

En cuanto a la segunda situación, es la que vamos a trabajar en el apartado A de la práctica.

El apartado B de la práctica se va a centrar en abordar cómo extraer evidencias cuando las máquinas virtuales se encuentran en instalaciones de terceros, como es el caso de Azure Cloud. En este caso, los volcados de memoria se obtendrán de la misma forma que estudiamos en clase el tema pasado. Asimismo se pueden lanzar scripts desde los cuales recolectar artefactos forenses interesantes para su posterior análisis. En cuanto a los discos duros virtuales podremos descargarlos o clonarlos en la nube para su análisis desde otra VM.

Objetivos:

- Tomar conciencia de las posibilidades que nos ofrece la nube a la hora de obtener evidencias forenses de máquinas virtualizadas.
- Extraer evidencias desde alguno de los sistemas en la nube más utilizados.

Materiales

- Cualquier distribución Windows que tengas virtualizada en tu/s sistema informático.
- Azure Cloud.
- Libcloudforensics

PARTE A: Extracción de evidencias On-premise

En este ejercicio práctico vamos a aprender cómo realizar un análisis forense de un equipo Windows virtualizado con VirtualBox. El objetivo es, como de costumbre, obtener un volcado de memoria y una imagen de disco de una máquina virtual Windows que está en ejecución, y posteriormente convertirlos a formatos compatibles con herramientas de análisis forense.

Para ello, sigue los siguientes pasos utilizando el comando VBoxManage:

1. Lee el siguiente artículo.

2. Abre una consola de comandos en tu sistema operativo y navega hasta el directorio donde se encuentra instalado VirtualBox.

3. Una vez en ese directorio, escribe el siguiente comando para listar todas las máquinas virtuales que tienes disponibles:

```
VBoxManage list vms
```

4. Identifica el nombre de la máquina virtual de la que deseas obtener el volcado de memoria y la imagen de disco, y anótalo.

5. Para realizar el volcado de memoria, ejecuta el siguiente comando:

```
VBoxManage debugvm <nombre de la máquina virtual> dumpvmcore --filename <nombre del archivo>
```

Este comando generará un archivo con extensión .dmp que contendrá el volcado de memoria de la máquina virtual especificada. Este archivo no es compatible con la mayoría de las herramientas de análisis forense, así que necesitamos convertirlo.

6. Para convertir el archivo .dmp a un formato compatible con herramientas de análisis forense, utiliza el siguiente comando:

```
volatility -f <nombre del archivo>.dmp imagecopy -O <nombre del archivo>.raw
```

7. Ahora, para obtener una imagen de disco de la máquina virtual, utiliza el siguiente comando:

```
VBoxManage clonehd <ruta del archivo de disco virtual> <ruta del archivo de destino> --format <formato de salida>
```

En el campo <ruta del archivo de disco virtual>, especifica la ubicación del archivo de disco virtual de la máquina virtual. En el campo <ruta del archivo de destino>, especifica la ubicación y nombre del archivo de destino que deseas crear. En el campo <formato de salida>, utiliza "raw" o "img" dependiendo del formato que necesites.

Una vez que hayas realizado el volcado de memoria y la imagen de disco, ya podrás utilizar herramientas de análisis forense para investigar y descubrir información importante de la máquina virtual analizada.

PARTE B: Extracción de evidencias desde Azure Cloud

1. Haciendo uso de tu cuenta de @ieszaidinvergeles.org, registrate en Azure Cloud en la siguiente URL:

   https://portal.azure.com/

2. Create una VM de tipo “debian 11” con las características que estimes oportunas, asegurándote de que la conexión SSH puerto 22 está activa. Pon la máquina a funcionar tomando nota de la IP de la misma y controlando las credenciales que se te faciliten.

3. Lee el siguiente enlace y aprende a cómo realizar una conexión remota desde tu máquina hacia la nube Azure usando el cliente Putty. Si usas Linux para conectar con tu máquina deberás seguir estas otras instrucciones.

4. Realiza un volcado de memoria de tu máquina debian alojada en Azure.

5. Lee el siguiente artículo sobre cómo realizar un clonado de un VHD alojado en Azure. Realiza los pasos necesarios y obtén una imagen de tu disco duro virtual en la nube. Documenta bien el proceso

6. Instala el Azure CLI y logueate en azure desde línea de comandos.

7. Por último, instala en tu PC el software de python “libcloudforensics” y úsalo para realizar un clonado de disco de tu VM. Los siguientes enlaces 1 y 2 te pueden servir de ayuda para ponerlo en marcha.