ANÁLISIS FORENSE

IES Mar de Cádiz
El Puerto de Santa María

RESUELTO – Crear perfil de Linux para poder analizar la captura de RAM de Clark

Análisis Forense

Curso de Especialización en Ciberseguridad

IES Mar de Cádiz – El Puerto de Santa María

Cádiz - Spain

RESUELTO – Crear perfil de Linux para poder analizar la captura de RAM de Clark

Para leer la captura de Clark deberemos crear un perfil para el sistema operativo Ubuntu 16.04, ya que Volatility no posee un perfil para este sistema operativo. Para ello deberemos de instalar una máquina virtual con el mismo sistema del cual queremos hacer el perfil.

Una vez instalada la máquina virtual, realizamos los siguientes pasos:

1.- Instalamos las cabeceras de Linux:

```
# apt-get install build-essential linux-headers-`uname -r`
```

2.- Instalamos la utilidad de *volatility dwarfdump*:

```
# apt-get install dwarfdump volatility-tools
```

3.- Tras instalar dwarfdump tendremos que acceder al directorio /usr/src/volatility-tools/linux, que es una carpeta que se crea cuando instalamos esta utilidad, y dentro de ella ejecutamos el siguiente comando para generar el módulo del perfil llamado *module.dwarf*:

```
# make
```

4. - Lo último que nos queda es crear el perfil. Para ello deberemos de crear un fichero comprimido que contenga el modulo que hemos creado, module.dwarf, y el fichero "/boot/System.map**".**

Para ello ejecutaremos el siguiente comando:

```
# zip Ubuntu_4.15.0-112-generic_profile.zip module.dwarf boot/System.map-4.15.0-112-generic
```

5.- Ya tenemos creado nuestro perfil, ahora deberemos de exportarlo a nuestra maquina Kali Linux, que es donde tenemos el Volatility. Una vez lo hayamos hecho, copiamos el perfil a la carpeta "/volatility/plugins/overlays/linux**" de nuestro Volatility:**

```
# cp Ubuntu_4.15.0-112-generic_profile.zip /volatility/plugins/overlays/Linux
```

6.- Vamos a ver si Volatility ha podido reconocer el nuevo perfil que hemos introducido. Para ello solo deberemos de ejecutar el siguiente comando y ver si está nuestro perfil:

```
# pyhton vol.py --info | greep Profile
```

Una vez que ya tenemos nuestro perfil integrado, podremos analizar la captura de RAM de Clark.
Ahora vamos a listar los procesos de la memoria de Clark y obtener el PID del proceso Nautilus. Para ello ejecutaremos el siguiente comando donde filtraremos el resultado para que solo nos salga el proceso de Nautilus:

```
# python vol.py -f Clark.raw --profile=LinuxUbuntu_4_15_0-142-generic_profilex64 linux_pstree | grep nautilus
```